International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

K.131

(01/2022)

SERIES K: PROTECTION AGAINST INTERFERENCE

Design methodologies for telecommunication systems applying soft error measures

Recommendation ITU-T K.131

Recommendation ITU-T K.131

Design methodologies for telecommunication systems applying soft error measures

Summary

Recommendation ITU-T K.131 describes the principles and design methods for soft error measures for equipment that makes up carrier telecommunications networks. It also describes basic configurations of telecommunication equipment, definitions and methods to determine reliability requirements and procedures for the design of equipment from the perspective of mitigation of failures caused by soft errors. Also included are methods to determine the areas, e.g., circuit blocks or circuit packs, requiring soft error measures in telecommunication equipment in order to conform to reliability requirements. The main design issues to be considered for soft error measures are described, as well as the actual design methods for the application of measures against soft errors and their effects. Finally, the reliability evaluation methods using theoretical calculations and tests of actual equipment are described to confirm the effect of the applied measures and conformity to reliability requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T K.131	2018-01-13	5	11.1002/1000/13454
2.0	ITU-T K.131	2022-01-13	5	11.1002/1000/14935

Keywords

Client signal, neutron irradiation testing, silent failure, soft error, SRAM, telecommunication equipment.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Highly integrated, miniaturized semiconductor devices are essential for the development of telecommunication equipment that makes up carrier telecommunication networks requiring large capacity, high functionality and high reliability. However, preventing the occurrence of soft errors in these semiconductor devices is not possible within commercial cost constraints. Accordingly, it is necessary to take measures to prevent soft errors that occur in semiconductor devices from causing failures in telecommunication equipment. When implementing soft error measures, it is necessary both to understand the characteristics of soft errors that occur in the semiconductor devices and to implement soft error handling measures at the device and equipment levels.

Since soft errors are very infrequent in each individual unit of telecommunication equipment, it is not necessary to implement excessive measures when the number of installed units is small. However, in networks comprising several thousand units of telecommunication equipment, several soft errors may occur throughout the entire network every day. Therefore, it is necessary to set reliability requirements regarding soft errors in consideration of the operating conditions of the equipment in the telecommunication network and then to implement soft error measures at the design stage to comply with those requirements.

Thus, a wide range of knowledge and skills for soft error measures are needed, from setting reliability requirements to configuration and operation of devices, as well as equipment. This Recommendation describes the methodology and procedures for designing equipment to mitigate failures caused by soft errors.

Recommendation ITU-T K.131

Design methodologies for telecommunication systems applying soft error measures

1 Scope

This Recommendation provides principles and appropriate methods for the design of measures to prevent failures caused by soft errors to satisfy the reliability requirement for telecommunication equipment installed at telecommunications centres for carrier networks, including that in core networks (link and node) and access networks. The principle used to set reliability requirements is described, but the values related to the requirements lie outside the scope of this Recommendation.

A similar methodology for the design of equipment made from dedicated hardware that configures physical network function-based networks described in this Recommendation may be applied to equipment made from general-purpose hardware that configures virtual network function-based networks expected to be introduced in the future. However, the precise methodology is still under study at the time of approval.

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 K.124] Recommendation ITU-T K.124 (2022), *Overview of particle radiation effects on telecommunication systems*.

[ITU-T K.130] Recommendation ITU-T K.130 (2022), *Neutron irradiation test methods for telecommunication equipment*.

[ITU-T K.139] Recommendation ITU-T K.139 (2022), *Reliability requirements for telecommunication systems affected by particle radiation*.

[ITU-T K.150] Recommendation ITU-T K.150 (2020), *Information of semiconductor devices required for the design of telecommunication equipment applying soft error mitigation measures.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 alert function reliability (AR): Reliability of equipment operation.

3.2.2 circuit pack: A circuit board that is inserted in a unit and easily changed by maintenance personnel.

3.2.3 error correction code correction; ECC correction: Automatic output of data corrected by logical processing using an error correction code (ECC) following identification of an erroneous bit.

3.2.4 failure in time (FIT): The unit that indicates the number of failures that can be expected in 10^9 h (one billion hours) of operation.

3.2.5 hardware failure: An abnormality in hardware that makes equipment operate improperly.

3.2.6 maintenance reliability (MR): Reliability of equipment maintenance.

3.2.7 non-signal effect block: Block that does not affect (impact) the client signal during soft error occurrences and reinitialization or other measures to recover from soft errors.

3.2.8 physical fault: A phenomenon in which a device physically deteriorates and causes malfunction.

3.2.9 physical fault failure: Hardware failures caused by physical fault.

3.2.10 service reliability (SR): Degree to which a service provides consistent and stable service outcomes.

3.2.11 signal effect block: Blocks that affect (impact) the client signal during soft error occurrences and reinitialization or other measures to recover from soft errors.

3.2.12 silent failure: A failure where no alert is issued to network operation equipment or maintenance personnel even though there is an effect on the client signal.

3.2.13 soft error: A phenomenon in which one or more bits within the data on the device have their values reversed. A soft error does not constitute damage to the actual device.

3.2.14 soft error failure: Hardware failures caused by soft error.

3.2.15 soft error failure rate (SEFR): Number of occurrences of failure in equipment caused by soft errors in devices divided by time.

3.2.16 soft error rate (SER): Number of occurrences of soft errors divided by time.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AR Alert function Reliability

ASIC Application Specific Integrated Circuit

ASSP Application Specific Standard Product

CPLD Complex Programmable Logic Device

CPU Central Processing Unit

CRAM Configuration Random Access Memory

CRC Cyclic Redundancy Check

DICE Dual Interlocked Storage Cell

DRAM Dynamic Random Access Memory

ECC	Error Correction Code
FinFET	Fin Field Effect Transistor
FIT	Failure In Time
FPGA	Field Programmable Gate Array
IC	Integrated Circuit
LSI	Large-Scale Integration
MCU	Multiple-Cell Upset
MLC	Multilevel Cell
MRAM	Magnetoresistive Random Access Memory
MR	Maintenance Reliability
OAM	Operations, Administration and Maintenance
PNF	Physical Network Function
RAM	Random Access Memory
RCC	Reinforcing Charge Collection
ROM	Read Only Memory
SCU	Single Cell Upset
SDH	Synchronous Digital Hierarchy
SER	Soft Error Rate
SEFR	Soft Error Failure Rate
SLC	Single Level Cell
SR	Service Reliability
SRAM	Static Random Access Memory
TLC	Triple Level Cell
TMR	Triple Modular Redundancy
ULA	Ultralow Alpha
WDT	Watchdog Timer

5 Conventions

None.

6 Basic configurations for telecommunication equipment

This clause describes the basic configurations of the telecommunication equipment that makes up carrier networks to be considered from the perspective of the effect of soft errors and measures to counteract them.

6.1 Basic functional configurations (classification of function blocks regarding effect on client signal)

Figure 6-1 shows the basic functional configuration of telecommunication equipment from the perspective of the effect of a soft error.

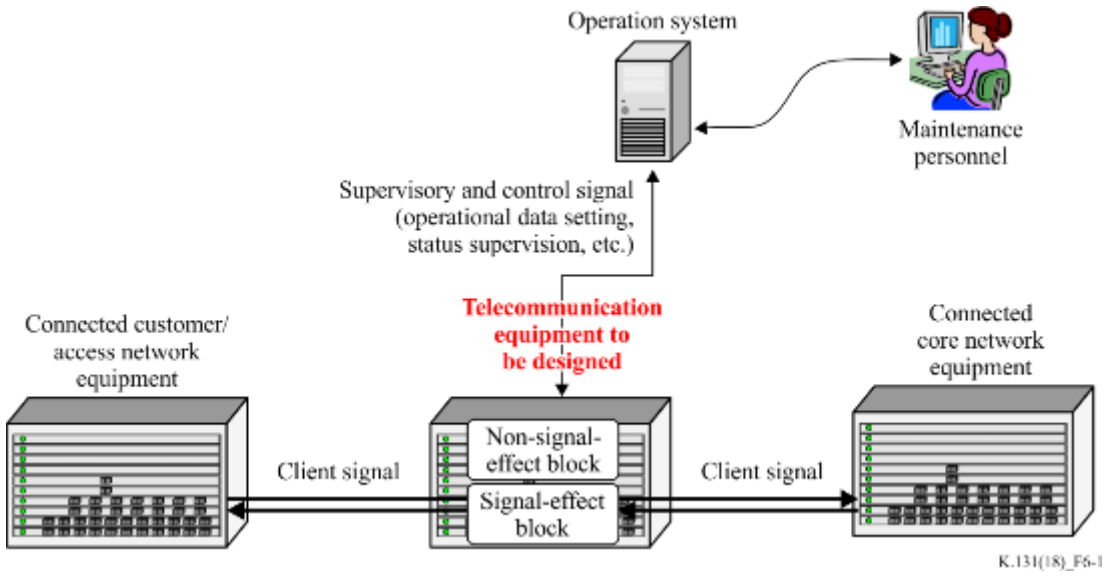

Figure 6-1 – Basic functional configuration of telecommunication equipment from the perspective of the effect of a soft error

The primary role of telecommunication equipment is to transmit client signals without errors in order to provide telecommunications services. The mitigation of the impact of failures caused by soft errors on services, such as an interruption to the client signal, is important in the design of countermeasures. To apply countermeasures during a soft error occurrence and the recovery operation such as reinitialization of the executed block, the basic function blocks of equipment should be classified into: signal effect blocks, where the client signal is affected; and non-signal effect blocks, where the client signal is not affected. An example of a signal effect block is a function block that sends and receives client signals to and from connected customer equipment, or access or core network equipment. Also included are function blocks for performing operations such as packet data routing and time-division data switching for transmitting client signal data. On the other hand, non-signal effect blocks include components that connect to the operation system via a maintenance personnel interface and send orders from the maintenance personnel to control equipment operational settings, such as path settings, circuit pack registration and state changes. It also includes components that notify maintenance personnel about supervisory information concerning equipment status such as failures or operational conditions.

6.2 Equipment configuration (components, circuit packs and unit)

Figure 6-2 shows the basic hardware configuration of telecommunication equipment.

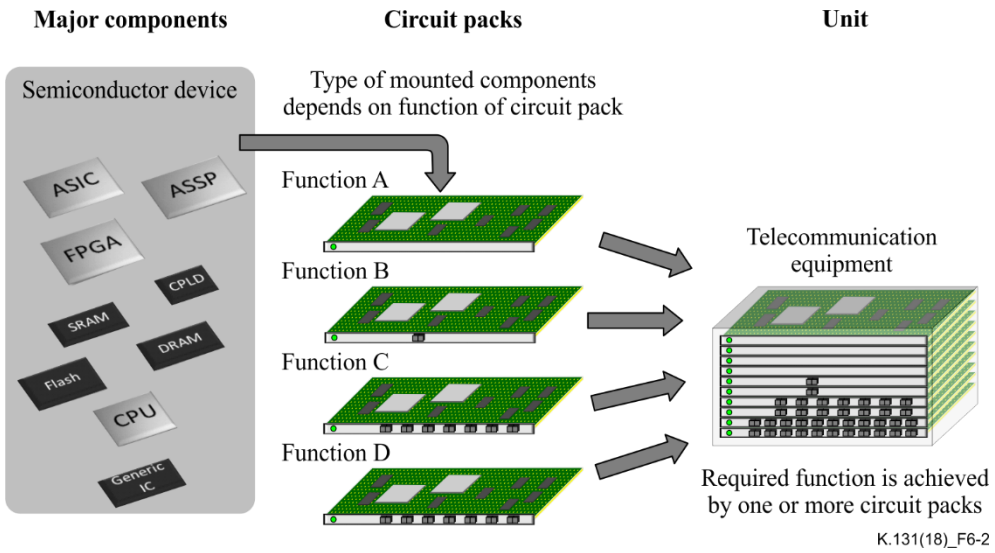

Figure 6-2 – Telecommunication equipment basic hardware configuration

The major components in this equipment are semiconductor devices, which readily generate soft errors. These devices are mounted in a circuit pack to achieve the required functionality. The telecommunication equipment consists of units comprising one or more circuit packs. When a hardware failure occurs in the telecommunication equipment, recovery is generally carried out by replacing the circuit pack.

6.3 Functional configurations to be considered for countermeasures

In this clause, the hardware configuration of the equipment and its functional configuration are clarified from the perspective of soft error countermeasures. It is essential to design soft error countermeasures considering the aspects described in clauses 6.3.1 to 6.3.3.

6.3.1 Allocation of basic function blocks in hardware

Figure 6-3 shows the allocation of basic function blocks in hardware. Depending on the scale of function blocks to be implemented, blocks that do or do not affect the client signal may be separated in one of the following ways: 1) as separate parts in a single device; 2) as separate devices within a single circuit pack; and 3) as separate circuit packs in a unit. For example, if a separate circuit pack 3) that does not affect client signal can be initialized without impact on another circuit pack that is processing the client signal; this does not affect service reliability (SR). Thus, during an equipment design process including soft error measures to meet SR requirements, it is essential to understand how the signal effect blocks are separated or integrated physically from non-signal effect blocks.

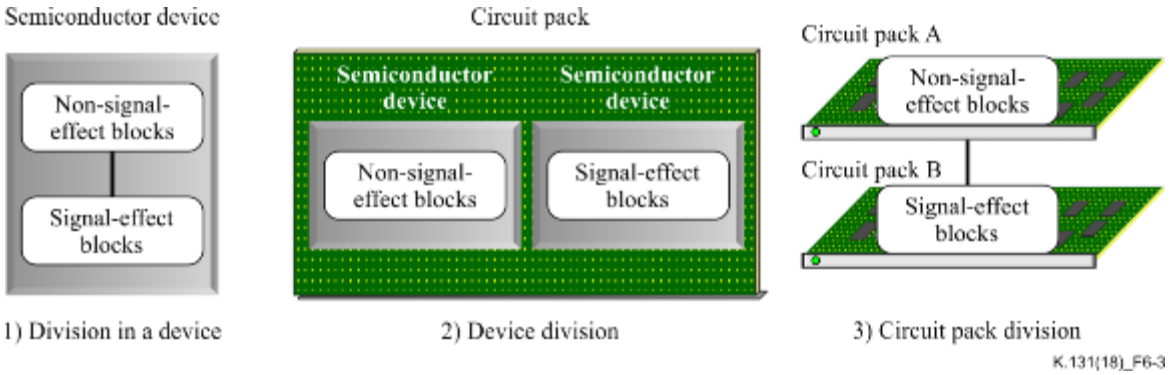

Figure 6-3 – Allocation of basic function blocks

6.3.2 Redundant configuration

Figure 6-4 shows redundant configuration. Redundant configuration is usually applied within the network or within the telecommunication equipment, according to the need to guarantee reliability, given the possibility of hardware failures. Even if soft errors occur, the network can remain in service by switching the path or system. The equipment in the inactive path or system can be restored while the other is active and measures to rectify soft errors can be undertaken without any impact on the service. Accordingly, in functional locations that have a redundant configuration, switchable units (such as paths, circuits, and circuit packs) and the changeover duration must be fully understood when designing these measures.

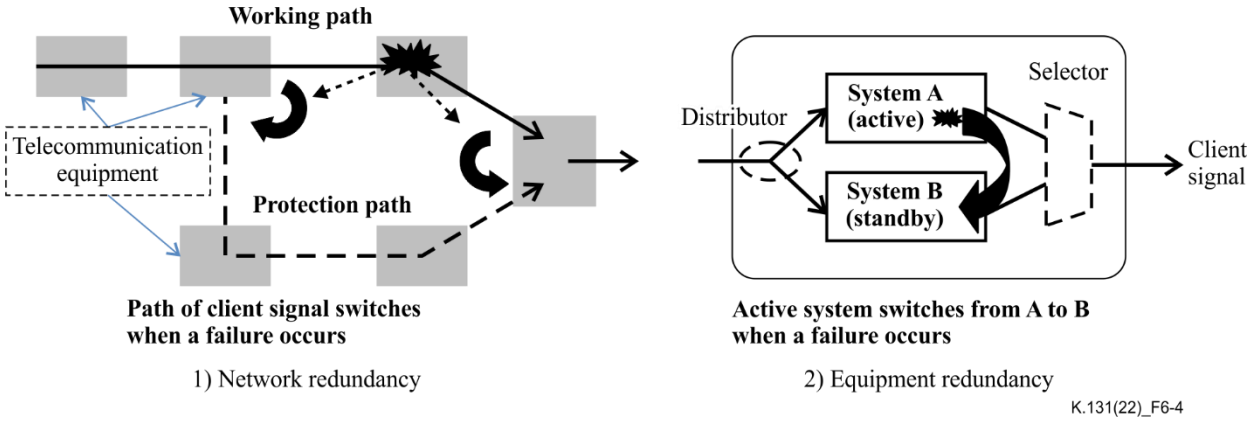

Figure 6-4 – Redundant configuration

6.3.3 Initial start-up configuration

Figure 6-5 is a general depiction of the initial start-up configuration. Data and programs required for the start-up of telecommunication equipment are normally stored in the non-volatile memory of the equipment. The data in the memory are not accessed for long intervals, since a restart of equipment for restoration or upgrading versions is very rare in telecommunication systems. Accordingly, if a soft error occurs in this memory and is not corrected appropriately; erroneous data may be stored for long periods in many pieces of equipment and are even provided upon restarting. Consequently, failures may occur in multiple pieces of equipment in operation when their system control programs are updated simultaneously or when the equipment is restarted for recovery from failure due to a major failure of the system. Failures on multiple pieces of equipment could lead to a shortage of circuit packs available for replacement. It is therefore important to evaluate the magnitude of the impact of stored erroneous data for start-up and apply measures to avoid unacceptable impact.

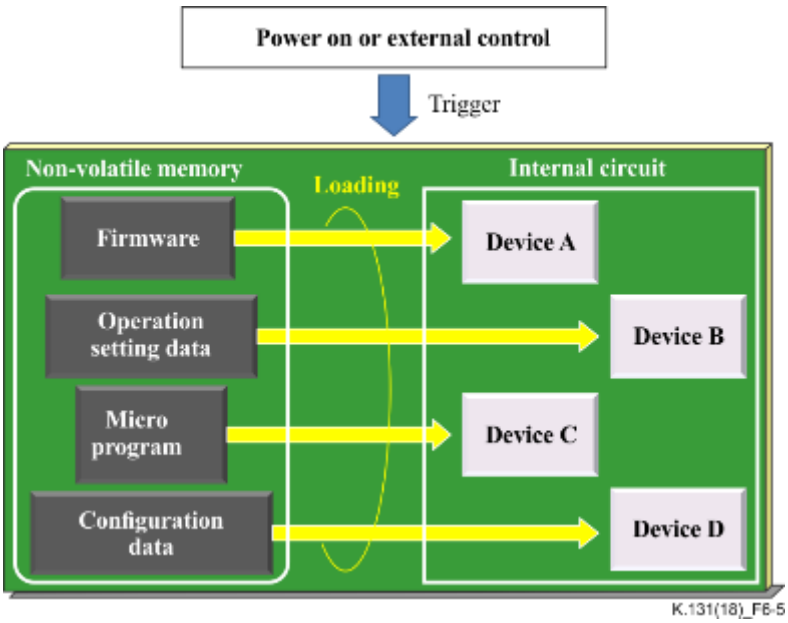

Figure 6-5 – Initial start-up configuration

7 Reliability requirements relating to soft errors and procedure of equipment design with mitigation measures

This clause specifies reliability requirements in terms of the soft error failure rate (SEFR) of telecommunication equipment and the procedure to develop mitigation measures for equipment to meet these requirements.

7.1 Reliability requirements

Figure 7-1 illustrates the procedure of recovery from physical fault failure and soft error failure when the measures described in clause 9 are correctly applied. Equipment reliability is determined by the possibility of incomplete recovery or occurrence of failures of unacceptable impact. This Recommendation specifies the reliability for three important steps in the recovery procedure.

The basic procedure is the same for physical fault failure and soft error failure, except that maintenance personnel must always perform restoration work for the former, whereas intervention by maintenance personnel is rarely required in the latter if soft error measures are adequately applied.

In the case of a soft error failure, the three types of reliability are determined based on three criteria:

1) whether it is possible to detect a failure and issue an alarm correctly;
2) whether the service can be restored in an acceptable time and the client signal can be handled properly;
3) whether the entire equipment can be restored automatically.

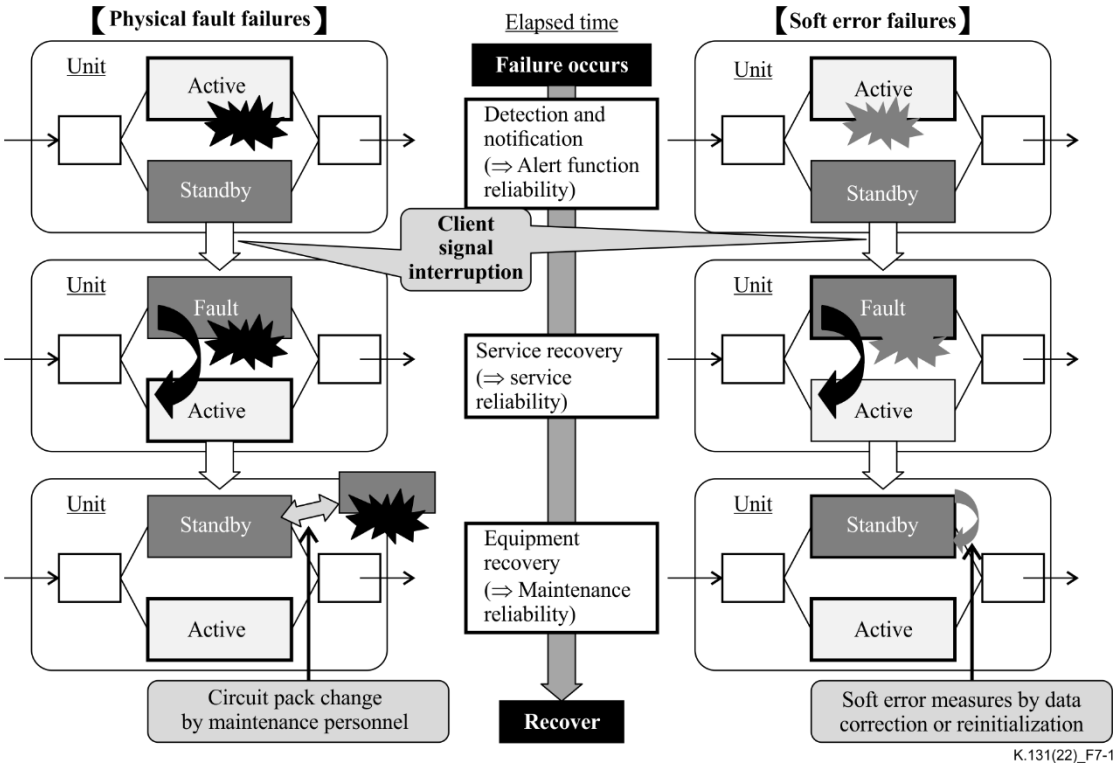

Figure 7-1 – Recovery procedure for physical fault failure and soft error failure

Table 7-1 lists the types of reliability requirements and their descriptions for telecommunication equipment within the scope of this Recommendation. The following three types of reliability requirements are specified in this Recommendation:

1) the alert function reliability (AR) requirement relating to equipment operation;
2) the SR requirement relating to service provision; and
3) the maintenance reliability (MR) requirement relating to equipment maintenance.

Some classes of reliability level are provided for each type of reliability requirement and the required reliability of the target equipment can be selected from the classes according to the conditions of the applicable network. Classes and values are described in [ITU-T K.139] for each type of reliability requirement described in Table 7-1.

Table 7-1 – Types of reliability requirements

Type	Abbreviation	Details
Alert function reliability requirements	AR	Requirements relating to equipment operation. Requirements are classified based on performance of failure detection and the issuing of an alert when a failure that impacts the client signals caused by a soft error occurs.
Service reliability requirements	SR	Requirements relating to service provision. Requirements are classified based on both the period and frequency of occurrences of a continuous interruption of client signals resulting from a soft error.
Maintenance reliability requirements	MR	Requirements relating to equipment maintenance. Requirements are classified based on the frequency of maintenance where maintenance personnel are required to carry out remote operation or on-site replacement of circuit packs to restore equipment after a soft error failure.

7.2 Equipment development procedures to implement mitigation measures

Figure 7-2 shows the issues for consideration when installing mitigation measures for soft error failures at each development stage.

First, the required reliability levels are determined by considering the services provided as well as the number of installed equipment units through examination of the specifications. Then, an applicable class within the reliability requirements shall be selected.

Next, during the design stage, the SEFR should be estimated through calculations and mitigation methods should be implemented to meet the requirements for the selected reliability class. The results are then examined by estimating the SEFR again. This procedure should be repeated until the result satisfies the specification.

Finally, tests on conformity to the reliability specification should be performed on real equipment through error injection to a semiconductor device or neutron irradiation test using a particle accelerator. After these tests, reliability is evaluated, and this should conform to the requirement.

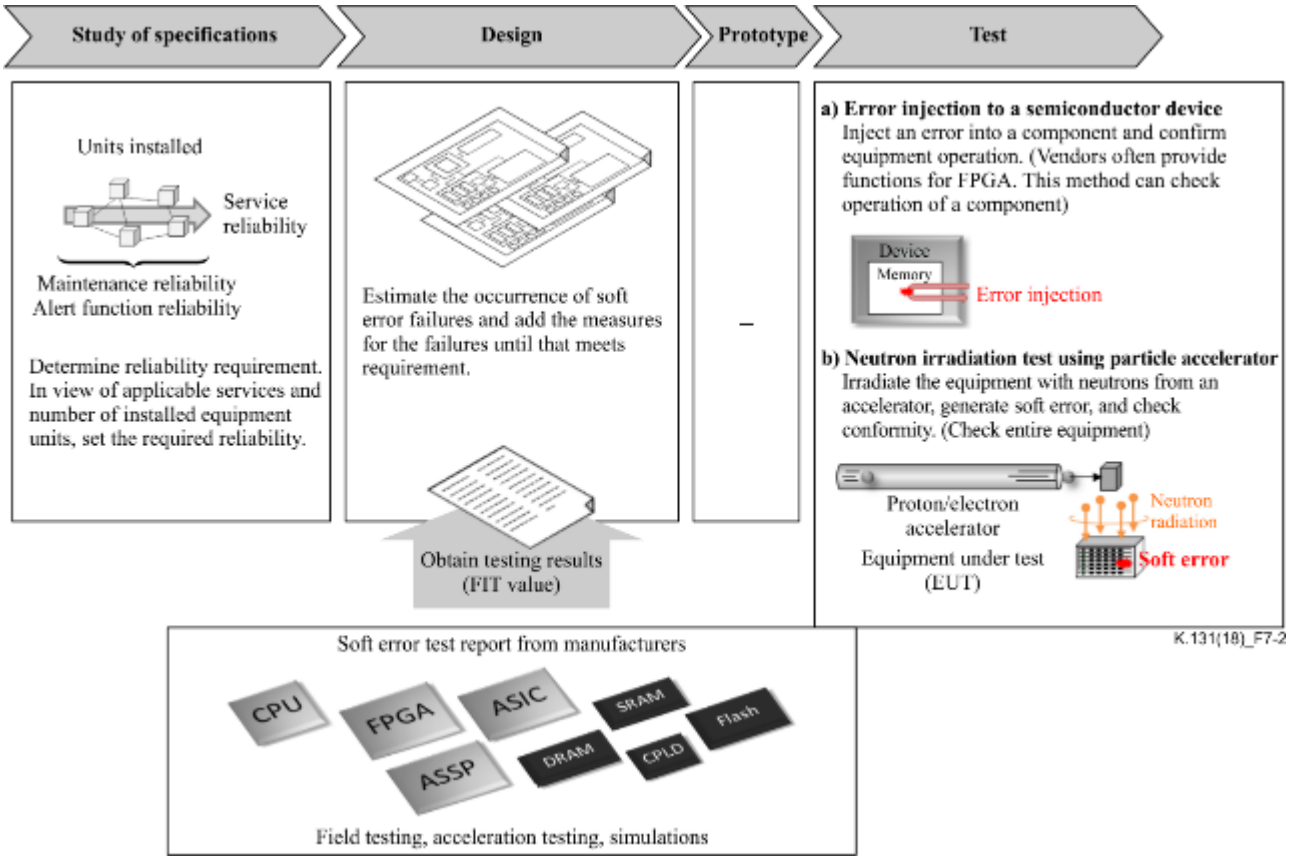

Figure 7-2 – Procedures for implementation of soft error measures in development of equipment

8 Estimation of soft error impact

This clause describes methods for estimating impacts by soft error and the SEFR for telecommunication equipment during the design stage.

8.1 Devices impacted by soft errors

8.1.1 Characteristics of semiconductor circuits in relation to soft error rate

Semiconductor devices, which are major components in telecommunication equipment and easily impacted by soft errors, mainly comprise memory circuits and logic circuits. The memory circuits

can be classified as: static random access memory (SRAM); dynamic random access memory (DRAM); and flash memory; the logic circuits can be classified as: sequential circuits; and combinational circuits. Table 8-1 shows the characteristics of each type of semiconductor circuit in relation to the soft error rate (SER).

Table 8-1 – Characteristics of semiconductor circuits in relation to soft error rate

<table>
<tr><th colspan="2">Circuit classification</th><th>Characteristics</th><th>SER</th></tr>
<tr><td rowspan="3">Memory circuit</td><td>SRAM</td><td>High speed
Uses flip-flop circuits as storage elements. Often used in applications requiring high speed.
Low capacity
Cannot be mounted with as high a density as DRAM and not suited for use as large capacity memory.
NOTE – Also used for configuration of random access memory (CRAM) to store field programmable gate array (FPGA) configuration data</td><td>High
SER is increased with miniaturization of large-scale integration (LSI) feature size</td></tr>
<tr><td>DRAM</td><td>Large capacity, volatile
Uses circuits that store a charge using capacitors and transistors as storage elements. Widely used as large capacity memory for main storage memory in computers.</td><td>Low
SER per memory capacity is low for structural reasons. The SER per memory capacity of DRAM is 10^{-3} to 10^{-4} times that of SRAM, but given the high density of DRAM components, the SER contribution can be significant.</td></tr>
<tr><td>Flash memory</td><td>Large capacity, non-volatile
A type of non-volatile semiconductor memory that can be overwritten and which retains data even when powered off.</td><td>Medium to low
SER per memory capacity is approximately 1/100 times that of SRAM. However, it is increasing because both NOR-type and NAND-type flash memory cells have been miniaturized with greater capacity and their structures have been changed from single level cell (SLC) to multilevel cell (MLC) and from MLC to triple level cell (TLC).</td></tr>
<tr><td rowspan="2">Logic circuit</td><td>Sequential circuit</td><td>A type of circuit that retains its internal status and determines output depending on external inputs and the internal status.
Examples: flip-flop, latch.</td><td rowspan="2">Medium to low
Generally, logic circuits have a high immunity to soft errors and at present, do not cause significant problems with soft errors in the field of telecommunications. However, moves towards miniaturization of feature sizes and lower power consumption are leading to an increase in soft errors.</td></tr>
<tr><td>Combinational circuit</td><td>A type of circuit that determines output depending on external inputs only.
Examples: inverter, NAND/NOR.</td></tr>
</table>

The miniaturization of feature sizes and higher operating speeds have resulted in an overall increase in SER per chip area. In particular, the probability of the occurrence of soft errors in SRAM is high, which is becoming a problem in telecommunication equipment. The probability of occurrence of soft errors is also increasing in flash memories and logic circuits, even though the current situation is not problematic, and it is necessary to pay attention to future trends (see Appendix I).

Recent progress in integration and microfabrication technologies has resulted in a dramatic increase in the occurrence of soft errors in contrast to hard errors, which permanently disable semiconductor devices. In particular, SRAM devices are easily affected by high-energy neutrons. Figure 8-1 shows the relationship between the design rule and failure in time (FIT) in the case of an SRAM-based FPGA [b-Iwashita].

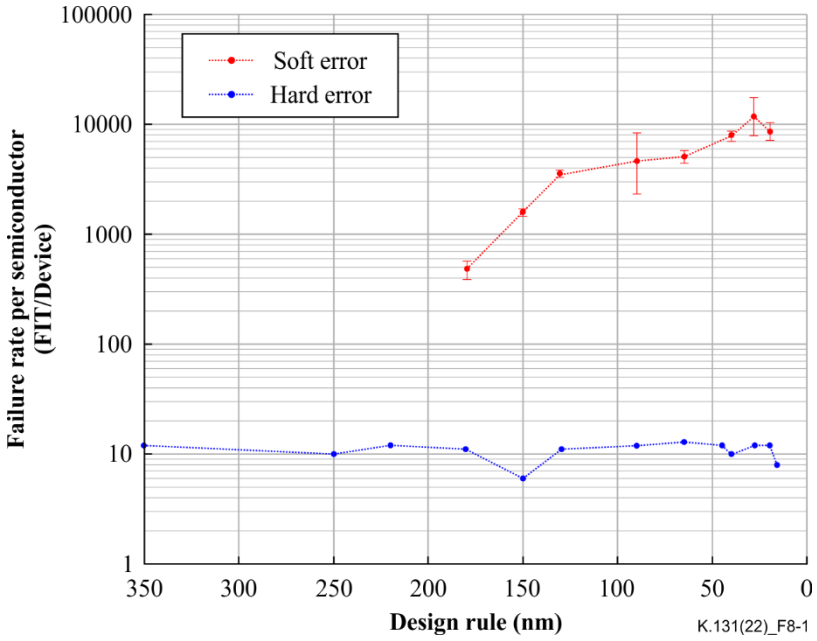

Figure 8-1 – Relationship between the design rule and FIT in case of an SRAM-based FPGA [b-Iwashita]

8.1.2 Types of circuits implemented in semiconductor devices

Table 8-2 shows the circuit types used in various types of semiconductor devices as major components. SRAM and logic circuits are used in most devices. Specifically, FPGA, which is the most common LSI used for telecommunication equipment, stores configuration data in SRAM to determine the circuit configuration so that any function can be realized. Since SRAM is heavily used in FPGA, FPGA vendors apply many types of countermeasures to the physical structure of FPGA, as well as providing design tools for equipment manufacturers to reduce failures caused by soft errors, see [b-ITU-T K-Suppl.11].

Table 8-2 – Types of circuits implemented in semiconductor devices

Semiconductor device	Memory circuit			Logic circuit	
	SRAM	DRAM	Flash memory	Sequential circuit	Combinational circuit
Application specific integrated circuit (ASIC)	✓	✓		✓	✓
Application specific standard product (ASSP)	✓			✓	✓
FPGA	✓		✓ (small scale only)	✓	✓
Complex programmable logic device (CPLD)	✓		✓	✓	✓
Random access memory/read only memory (RAM/ROM)	✓	✓	✓		
Central processing unit (CPU)	✓			✓	✓
Generic integrated circuit (IC)				✓	✓

8.1.3 Soft error impact relating to SRAM usage form

There are differences in the impact of soft errors on operation depending on the usage of SRAMs in equipment. SRAM usage can be classified into three types: setting data storage memory, operation

control memory and data buffer memory. Table 8-3 summarizes the operation, soft error impacts and concrete usage examples for each of these usage conditions.

Table 8-3 – Soft error impact relating to SRAM usage form

Usage type	Outline of operation	Soft error impacts without mitigation	Usage example
Setting data storage memory	After data are written, only data retention and readout operations are performed	**Large** Since there is no opportunity to restore erroneous data after data are written, the impact on equipment operation is ongoing.	Operating parameters Switching information Configuration data Firmware Micro program
Operation control memory	Since readout and writing operations are repeated, erroneous data are temporarily used but do not remain in memory for long	**Large** Use of erroneous data may cause subsequent impact on operation.	Client signal operation control CPU cache
Data buffer memory		**Small** Intermittent data errors. Degree of impact depends on the equipment configuration and services provided.	Client signal buffer Control signal transmission/reception buffer

Soft errors in setting data storage memory or operation control memory have a major impact on functionality, so there is a strong requirement for soft error countermeasures. Soft errors in data buffer memory are temporary and the impact is limited to the data upon which the errors occurred, because correct new data regularly replace the erroneous ones. Accordingly, even if soft error measures are not implemented, normal conditions are restored after a single bit, packet, or frame interruption on the client signal, and this has a minor impact on SR. However, if there is a possibility that erroneous data could leak out to other areas and affect functionality, countermeasures may be required. Additionally, if a service does not permit these types of single client signal interruptions, countermeasures are required to make it possible for the reversed data to be corrected when data are retrieved.

8.2 Estimation method for soft error failure rate

In hardware design, the SEFR should be estimated using the following procedure based upon the characteristics of semiconductor devices regarding soft errors as described in clause 8.1, when the devices to be used for the equipment are selected.

Figure 8-2 shows an example of a circuit configuration diagram using semiconductor devices in a circuit pack. Based on Figure 8-2, the designer should then create an itemized list of components and their circuit types based on soft error occurrence. An example is shown in Table 8-4.

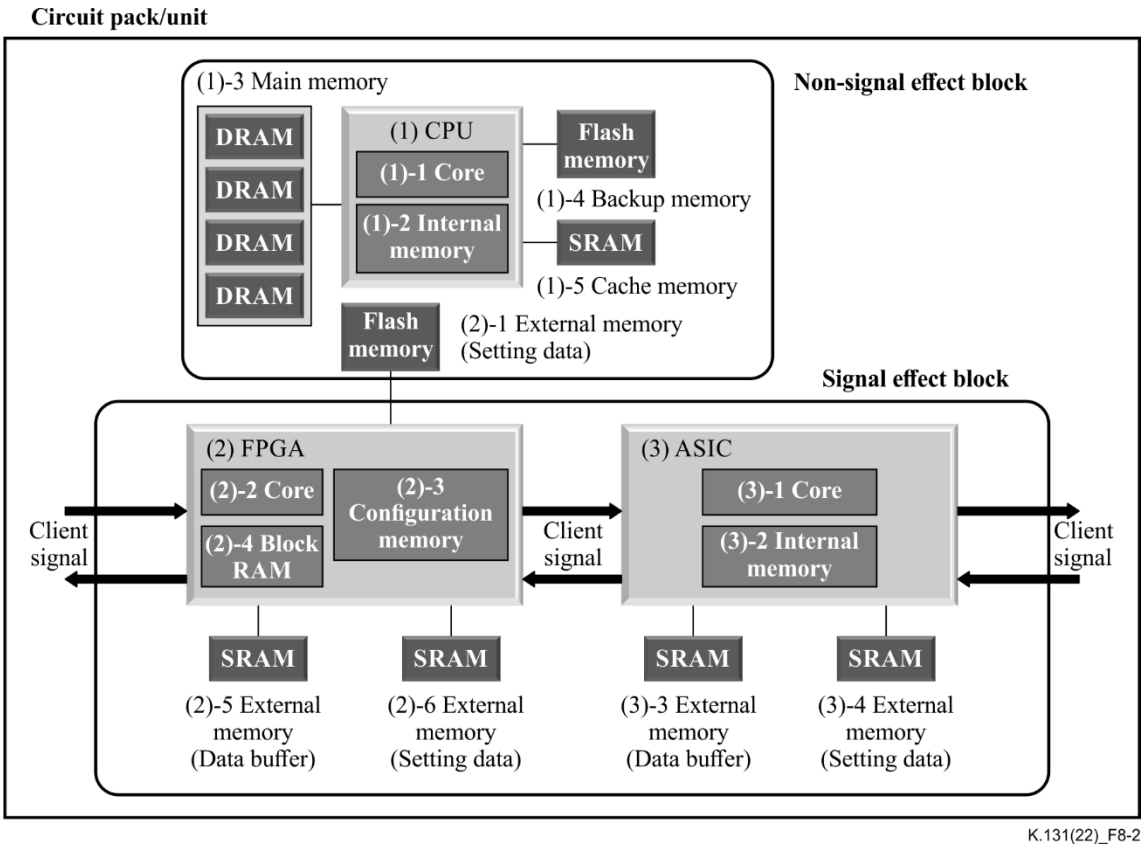

Figure 8-2 – Example of identifying devices impacted by soft errors

Table 8-4 – Example of estimation items for soft error failure rate

Impact on client signal when the function block fails (Figure 6-1)	**Type**		**Functions/usage conditions**	**Circuit classification**	**SEFR calculation (FIT)**	
					Service reliability requirement	**Maintenance reliability requirement**
No impact	(1) CPU peripheral circuit	1	Core	Logic circuit	N/A	To be determined
		2	Internal memory (operation control, setting data, data buffer)	SRAM		
		3	Main memory (operation control, setting data, data buffer)	DRAM		
		4	Backup memory (setting data)	Flash memory		
		5	Cache memory (operation control)	SRAM		
	(2) FPGA peripheral circuit	1	External memory (setting data)	Flash memory		
Impact		2	Core	Logic circuit	To be determined	
		3	Configuration memory (setting data)	SRAM		

Table 8-4 – Example of estimation items for soft error failure rate

Impact on client signal when the function block fails (Figure 6-1)	Type		Functions/usage conditions	Circuit classification	SEFR calculation (FIT)	
					Service reliability requirement	Maintenance reliability requirement
		4	Block RAM (operation control, setting data, data buffer)	SRAM		
		5	External memory (data buffer)	SRAM		N/A
		6	External memory (setting data)	SRAM		To be determined
	(3) ASIC peripheral circuit	1	Core	Logic circuit		
		2	Internal memory (operation control, setting data, data buffer)	SRAM		
		3	External memory (data buffer)	SRAM		N/A
		4	External memory (setting data)	SRAM		To be determined

The SEFR for each item should refer to the vendor-supplied values measured by the method in conformance with the standards usually referenced by the manufacturers. If values have not been published, equipment design vendors need either to obtain information separately from device vendors or estimate values from the characteristics of similar devices. As an example, published values for FPGAs from Xilinx can be found in [b-Xilinx], but the values only incorporate mitigation methods at the individual device level regarding soft errors. Accordingly, designers should estimate the soft error failure rate before implementing mitigation methods at the equipment level, accounting for memory usage and equipment configuration as shown in Table 8-4. [ITU-T K.150] clarifies characteristic parameters necessary for design of soft error mitigation measures in telecommunication equipment that are expected to be supplied from semiconductor device vendors. If the equipment comprises multiple circuit packs and types of circuit pack, the occurrence rate for a piece of equipment can be calculated as the total value of all circuit packs. Devices or circuit blocks where mitigation methods are needed should then be identified from the calculated occurrence rate and required reliability.

The total SEFR should be calculated separately for SR and MR. SR calculations should only be performed for components that impact the client signal. On the other hand, MR calculations should be performed for all components that may perpetuate failure conditions caused by soft errors, regardless of the affected function. Furthermore, since soft errors that occur in data buffer memory are temporary, this is not included in the SEFR for MR.

9 Methods for implementation of soft error measures

This clause describes methods for the implementation of failure mitigation measures against soft errors in equipment to conform to the specified requirements for the reliability class selected in the study of specifications.

9.1 Principles of mitigation measures

There are three principles of soft error measures: reduction; isolation; and correction. Table 9-1 lists methods for the implementation of soft error measures and specific examples for each perspective.

Table 9-1 – Principles of soft error measures

Principles	Mitigation techniques		Examples
Reduction	1	Change in materials	Magnetoresistive random access memory (MRAM) Ultralow alpha (ULA) particle-emitting package materials
	2	Work on physical structure	3D transistor structure (fin field effect transistor (FinFET), etc.) reinforcing charge collection (RCC) technology for logical circuits
	3	Reduction in areas where soft errors occur	Elimination of CRAM by use of ASIC instead of FPGA
Isolation	1	Work on circuit configuration	Triple modular redundancy (TMR) Memory bit interleaving configuration
	2	Identification of parts with and without substantial function	Remove monitoring of areas where RAM is unused. Remove parts that are not active in CRAM of FPGA from monitoring target.
Correction	1	Automatic correction in hardware	Error correction code (ECC) correction or corrected data overwriting Dual interlocked storage cell (DICE) structure logic circuit
	2	Automatic correction in the equipment control program	Setting data overwriting Reinitialization
	3	Correction in accordance with maintenance personnel operation	Reset by remote control

9.1.1 Reduction

The reduction principle means using physical measures to reduce the occurrence of actual soft errors in a device. The measures include using devices such as magnetic materials that do not generate soft errors in contrast to semiconductor devices. The soft errors caused by alpha particles can also be reduced by use of a ULA material, which emits few of them, for semiconductor packages. Using a 3D transistor structure, in FinFET for example, the area susceptible to entering neutrons can be reduced. Using RCC technology, the charges generated by collision of fast ions with the silicon are absorbed with a dummy inverter circuit and the occurrence rate of soft errors is reduced. The reduction in the amount of SRAM susceptible to neutron irradiation can reduce the occurrence of soft errors. Soft error reduction can be implemented physically by selection of devices at the equipment design stage. Consequently, the estimation of SEFR according to Table 8-4 is conducted assuming that physical measures have already been incorporated.

9.1.2 Isolation

The isolation principle means isolating the component in which a soft error occurred, so that it does not impact the reliability of the equipment. These measures include adoption of a configuration of TMR that enables continued operation by isolating the module with a soft error or use of an interleaved memory configuration to lessen the impact on the multiple cell upset (MCU). Maintenance efforts can also be reduced by identifying whether soft errors have any functional effect

and then suppressing or classifying the issuing of notices or alarms. Isolation measures are implemented at both the circuit design and the control program design levels.

9.1.3 Correction

The correction principle means automatic rectification of the data where a soft error occurred either by overwriting it with the correct information or reinitializing the whole data set to restore a normal state. This measure is effective since a soft error is not physical fault of the semiconductor device itself, but instead consists of a bit reversal in the data on this device.

Three kinds of operation or triggering methods are applied, namely, automatic correction in the hardware operation, correction triggered by automatic control in the equipment and correction triggered by maintenance personnel action.

Automatic correction in hardware operation is generally implemented using ECC correction and a data overwriting function that replaces erroneous memory circuits with corrected information. A DICE structure that repairs soft errors occurring within a latch in the structure is very tolerant to soft errors. The control program triggers the application of correction procedures when an error that can be rectified automatically is detected. However, for errors presenting a risk of major impact on services, maintenance personnel must apply the correction procedure after checking the degree of impact of the detected error and determining the procedure with the least risk to the recovery operation. Only the application of this method shall be counted for estimation of MR.

All these measures consist of two stages: detection and correction. Soft error detection and correction methods for soft error measures are described in clauses 9.2 and 9.3, respectively. Clauses 9.4 to 9.6 report examples of methods for soft error correction measures by combining detection and correction methods in SRAMs, in which soft errors easily occur. Impacts on the service and the MR are also described for each measure. Clause 9.7 describes so called "silent" failures that occur without warning, which have a major impact on services since no action can be initiated even if a function abnormality occurs in the equipment. Silent failures are counted in the estimation of the AR.

Measures using detection and correction are implemented at the circuit and control program design levels.

9.2 Soft error detection method

To initiate correction of soft errors when they occur through linkage to the hardware, the equipment control program or maintenance personnel, as described in clause 9.1.3, soft errors must first be detected within the equipment. Table 9-2 lists soft error detection methods.

Table 9-2 – Soft error detection methods

Classification of the detection method	Detection method	Characteristics (advantages/disadvantages)
Redundant bit addition	Parity check	Only effective for odd numbers of bit errors
	Cyclic redundancy check (CRC)	Detection of multiple bit errors is possible.
	Error correction code (ECC) check	Detection of single or two-bit errors is possible The position of the erroneous bit can be determined in the case of a single bit error.
Redundant circuit	Redundant circuit output data verification (dual modular redundancy)	Effective only for error detection It is not possible to determine which circuit has the error.
Health check	Watchdog timer (WDT) surveillance	Program runaway as a result of a bit error can be detected.
	Operations, administration and maintenance (OAM) data transmission/reception	Detection is possible even if there is no transmission/reception of valid data such as client or control signals.
	Periodic memory readout	Effective in detecting errors in memory accessed occasionally when needed Early detection of errors is possible before access of the memory.

Soft error detection methods can be classified into those using redundant bit addition, a redundant circuit or a health check. These methods are similar to those for physical fault failure detection. The cause of the failure can be determined by checking whether restoration can be done by the corrections described in clause 9.3.

In the redundant bit addition method, errors can be detected by adding redundancy to each data unit of client and control signals in accordance with a specified rule and then checking the consistency of the data to the rule. The redundant bit addition method includes the parity code check that can detect an odd number of bit errors (almost all odd numbers of bit errors are single for soft errors), the CRC that can detect multiple bit errors and ECC methods that can detect 1 or 2 bit errors. The position of the erroneous bit can be determined by an ECC check for a single error. The maximum number of bit errors that can be detected and the maximum number of bit errors for which the location can be determined by an ECC check are increasing with the successive improvements being made to the ECC check method. These methods are effective in detecting memory circuit errors.

In the redundant circuit method (dual modular redundancy), the same data are put into two identical circuits and the outputs are continuously compared to ensure the data are correct. This method can detect when an error occurs, but it cannot determine the circuit in which the error condition exists. This method is effective in detecting logic circuit errors.

A health check is conducted by monitoring from an external circuit to determine whether the equipment is operating correctly. Health check methods include WDT surveillance, OAM data transmission and reception and periodic memory readout. WDT surveillance periodically runs a program that resets the hard timer and detects malfunctions from a timeout signal generated by the timer when the program does not operate. This method is effective in detecting program runaway. Under the OAM data transmission and reception method, test data are periodically transmitted to and from function blocks at the end of the path of valid data such as client and control signals to check the health of the path. Surveillance is still possible even if there is no transmission and reception of the valid data. From the periodic memory readout, malfunctions in the memory readout function, as well as errors in memory cells, can be detected if data with redundant bits as described earlier are stored in the memory. This method is therefore effective in detecting errors in occasionally accessed memory and for early detection of errors prior to access.

9.3 Soft error correction method

Table 9-3 lists soft error correction methods. Unlike physical fault failures, operation of the equipment can be returned to a normal state by correction of erroneous data such as overwriting with correct data where the error occurred or by reinitialization.

Table 9-3 – Soft error correction methods

Classification	Correction method	Operation	Details
Data correction	ECC correction	Hardware	Identifies the erroneous bit from the outputs data and then corrects it by logical processing using ECC
	Corrected data overwriting	Hardware	Identifies the erroneous bit then overwrites the data corrected by logical processing in the same place in the memory space
	Setting data overwriting	Control program	Overwrites the original data stored in a memory that has high soft error immunity such as flash memory
Reinitialization	Circuit pack reset	Control program or maintenance personnel	Overall circuit pack reinitialization
	Device reset		Reinitialization of the relevant device only. Requires a shorter time for correction than circuit pack reset, but coordination with peripheral circuits is necessary
	FPGA reconfiguration		Data reread from flash memory or status matching with peripheral circuits may be necessary
	CPU reboot		Program initialization

The methods classified in data correction include: ECC correction, corrected data overwriting and setting data overwriting. ECC correction overwrites only output data but not memory data. ECC correction and corrected data overwriting automatically correct data by a logical process installed in hardware and setting data overwriting is initiated by the control program to overwrite by correct data that are stored separately. All these methods are applied to memory circuits. The number of correctable bits is limited by the application of ECC correction and corrected data overwriting, whereas setting data overwriting can correct all data. Additionally, the numbers of bits for which errors can be corrected are increasing with each generation of development through successive improvements in the check and the correction method.

Methods of reinitialization can be classified as: circuit pack reset; device reset; FPGA reconfiguration; and CPU reboot from the reinitialization range. The circuit pack reset method can be implemented rather easily since the reinitialization range is coincident with that of the maintenance unit. Device reset and FPGA reconfiguration can reduce the time for correction, but it is necessary to coordinate the operation with peripheral circuits in order to continue normal operation. Control methods for this correction processing may be carried out automatically by a control program or manually by maintenance personnel. If there is a possibility that the impact on services cannot be ignored at the time of reinitialization, maintenance personnel should evaluate the degree of impact and decide whether to initiate correction.

9.4 Example of soft error correction measures for setting data storage memory

Table 9-4 lists examples of soft error correction measures for setting data storage memory.

Table 9-4 – Examples of soft error measures for setting data storage memory

No	Soft error detection method	Soft error correction method	MCU measures	Impact on service reliability	Impact on maintenance reliability
1	Parity check	Setting data overwriting	No	Yes	No
2	Parity check	CPU reboot	No	Generally, no impact (depends on configuration of equipment)	No
3	CRC	Setting data overwriting	Yes	Yes	No
4	ECC check	ECC correction or corrected data overwriting	No	No	No
5	ECC check	ECC correction or corrected data overwriting (for single cell upset (SCU)) + setting data overwriting (for MCU)	Yes	Yes	No
6	ECC check (when memory has a bit interleaving structure)	ECC correction or corrected data overwriting	Yes	No	No

If the only detection method installed in the memory does not have a correction function, such as parity and CRC, a measure to overwrite setting data stored in a separate non-volatile memory should be applied.

If the failure rate by the MCU does not satisfy the required reliability class even though it adopts a method with an error correction function such as ECC correction and corrected data overwriting, restoration from the MCU should be performed by setting data overwriting. Furthermore, ECC correction is possible even for the MCU if memory with a bit-interleaved configuration is used.

It is possible to recover from the soft error with a reboot, if a parity error is detected in a CPU.

9.5 Examples of soft error correction measures for operational control memory and logic circuits

Table 9-5 lists examples of soft error correction measures for operational control memory and logic circuits.

Table 9-5 – Examples of soft error correction measures for operational control memory and logic circuits

No	Soft error detection method	Soft error correction method	MCU measures	Impact on service reliability	Impact on maintenance reliability
1	Parity check	Device/circuit pack reset	No	Yes	No
2	Parity check	Remote reset control	No	Yes	Yes
3	Parity check	CPU reboot	No	Generally, no impact (depends on configuration of equipment)	No

Table 9-5 – Examples of soft error correction measures for operational control memory and logic circuits

No	Soft error detection method	Soft error correction method	MCU measures	Impact on service reliability	Impact on maintenance reliability
4	CRC	Device/circuit pack reset	Yes	Yes	No
5	CRC	Remote reset control	Yes	Yes	Yes
6	ECC check	ECC correction or corrected data overwriting	No	No	No
7	ECC check	ECC correction or corrected data overwriting (to SCU) + Device/circuit pack reset (to MCU)	Yes	Yes	No
8	Duplicate circuit output data verification	Remote reset control	Yes	Yes	Yes
9	WDT	CPU reboot	Yes	Generally, no impact (depends on configuration of equipment)	No
10	OAM data transmission and reception	Device or circuit pack reset	Yes	Yes	No

If the only detection method installed in the memory does not have a correction function, such as parity and CRC, a measure such as resetting the device or circuit pack may be applied at the time of error detection. However, if the reset results in an interruption to the client signal that cannot be ignored, the SEFR must be evaluated to check the conformity to the SR requirement. If the reliability requirement is not satisfied, correction measures, e.g., use of ECC, corrected data overwriting and redundant configuration, should be improved to meet the requirement.

If the failure rate due to the MCU does not satisfy the required reliability class even though it adopts a method with an error correction function such as ECC correction and corrected data overwriting, restoration from the MCU should be performed by a reset of the relevant device or circuit pack.

The method where the maintenance personnel initiate a remote reset control at the time of error detection may be applied provided the MR estimated from the SEFR satisfies the requirement.

Additionally, in logic circuits that cannot use error detection codes such as parity codes, malfunctions can be detected by verification using the output of duplicate circuits or error detection with OAM data. A device or circuit pack reset should then be performed to recover from the soft error. In case of duplicate circuit output data verification, the discretion of maintenance personnel is required as it is not possible to determine which circuit has the error.

CPU recovery from a soft error may be performed by a reboot if an error is detected by using parity codes or a WDT.

9.6 Example of soft error measures for buffer memory

As discussed in clause 8.1, buffer memory is regularly overwritten with new, correct data, which means that the impact of soft errors in such memory is temporary. There is little impact on reliability even if no soft error measures are taken. Examples of measures to prevent outflow of erroneous data

and short signal interruption of client signals are presented in Table 9-6. In principle, ECC measures are recommended and MCUs can be mitigated by a combination of bit interleaving and ECC.

Table 9-6 – Examples of soft error measures for buffer memory

No	Soft error detection method	Soft error correction method	MCU measures	Impact on service reliability	Impact on maintenance reliability
1	ECC check	ECC correction	No	No	No
2	ECC check (when memory has a bit-interleaved structure)	ECC correction	Yes	No	No

9.7 Definition and consideration of silent failure

This Recommendation defines a silent failure caused by a soft error as a failure that cannot be reported to the carrier network operation system or maintenance personnel even though the failure causes a non-negligible impact on the client signal, as described in clause 7.2 of [ITU-T K.124]. There may be a report from the user before maintenance personnel are aware of the failure.

9.7.1 Configuration of failure monitoring function for client signals in carrier network

Figure 9-1 depicts internal connections related to the client signal among customers connected to the carrier network.

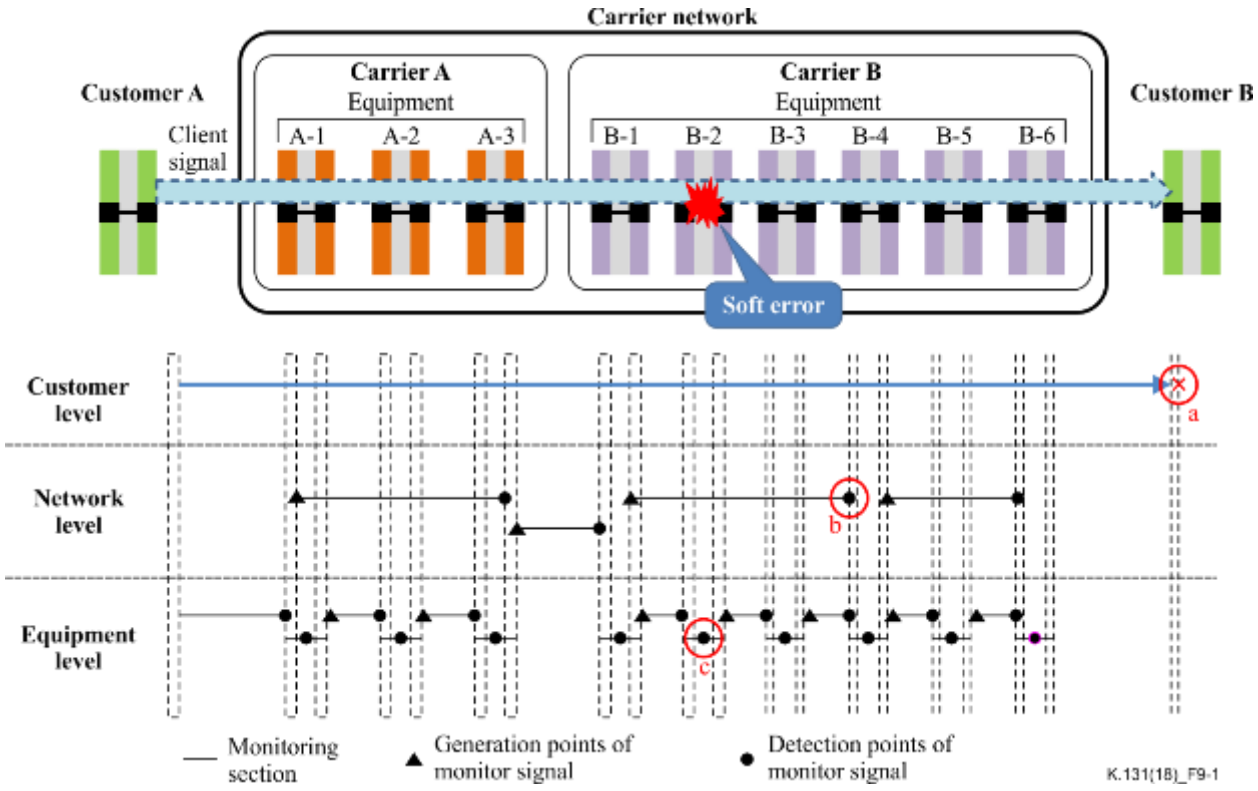

Figure 9-1 – Normality monitoring function in carrier network for client signal

Figure 9-1 shows the transmission pass of a client signal from customer A to customer B and several pieces of equipment within each carrier network. In addition, Figure 9-1 shows the general configuration of the error-monitoring function for the client transmission signal by using both

network level monitoring for each transmission path and equipment level monitoring for each piece of equipment.

Monitoring at the network level is performed by synchronous digital hierarchy (SDH) format transmission with overhead added to the client signal or transmission of an OAM packet on the client signal route. In this case, it is impossible to identify a piece of equipment in a failure state when multiple pieces of equipment are included in the monitoring path, since the signal fails if a failure occurs in any part of the equipment between the detection and generation points of the monitored signal. On the other hand, a piece of equipment in a failure state can be identified by the equipment level monitoring that incorporates a function to detect a malfunction in the piece of equipment and signal from the neighbouring equipment.

9.7.2 Relationship between silent failure and alert function reliability

This clause describes an example of a silent failure in the network having the configuration shown in Figure 9-1.

Suppose that a soft error has occurred in the piece of equipment labelled B-2 and an abnormality is detected by customer B. In this case, if an abnormality is detected and reported at point b at the network level and point c at the equipment level, then the piece of equipment in a failure state can be identified as B-2. In this case, it does not correspond to a silent failure and this failure is not counted as a failure for AR. On the other hand, if no abnormality is detected at points b and c, it is regarded as a silent failure, and this is counted in the AR evaluation of B-2.

When the case detection is made at point b, but not at point c, it is not classified as a silent failure if the definition is applied strictly, but the specific piece of equipment in a failure state cannot be determined and it takes time to identify it. Since this case may cause a major impact on service and maintenance, this may be similar to a silent failure. Therefore, the criteria to be counted in the AR evaluation should be determined by agreement between the equipment manufacturer and the carrier to install it.

9.7.3 Notes on the design to prevent silent failure

The following should be considered when implementing measures to prevent silent failures during equipment design.

a) The parity check measures which have been generally used have recently become less effective to prevent silent failures, since the occurrence of multi-bit errors which cannot be detected by the measure is getting more frequent.

b) In a failure caused by a soft error, unlike a physical fault failure from deterioration of parts, the area of the failure is usually limited to 1 bit of memory, one logic gate or one wire. Therefore, it may be difficult to cover all failure patterns in the design to implement the function abnormality detection circuit. This characteristic is significant especially in an FPGA that sets a circuit configuration using data in a CRAM. Since CRAM usage is generally about 10% to 20%, the majority of bit inversion in CRAM from soft errors occurs in the unused portion, which does not affect any functionality. Therefore, alarm notification by CRAM error detection is not performed on the equipment and a countermeasure may be taken by implementing an abnormality detection circuit using another function.

10 Notes on application of soft error measures

This clause notes equipment design considerations for soft error measure application.

10.1 Soft error measures for a redundant configuration function block

As described in clause 6.3.2, soft error measures utilizing a redundant configuration are performed basically by switching the path of customer signal to the redundant path immediately after any soft

error is detected that cannot be corrected without service interruption with a measure such as ECC correction. Equipment that is in a failure state can then be recovered by error correction such as reinitialization.

However, if signals of multiple clients are in operation in function blocks on a circuit pack as shown in Figure 10-1, the following additional procedures should be considered.

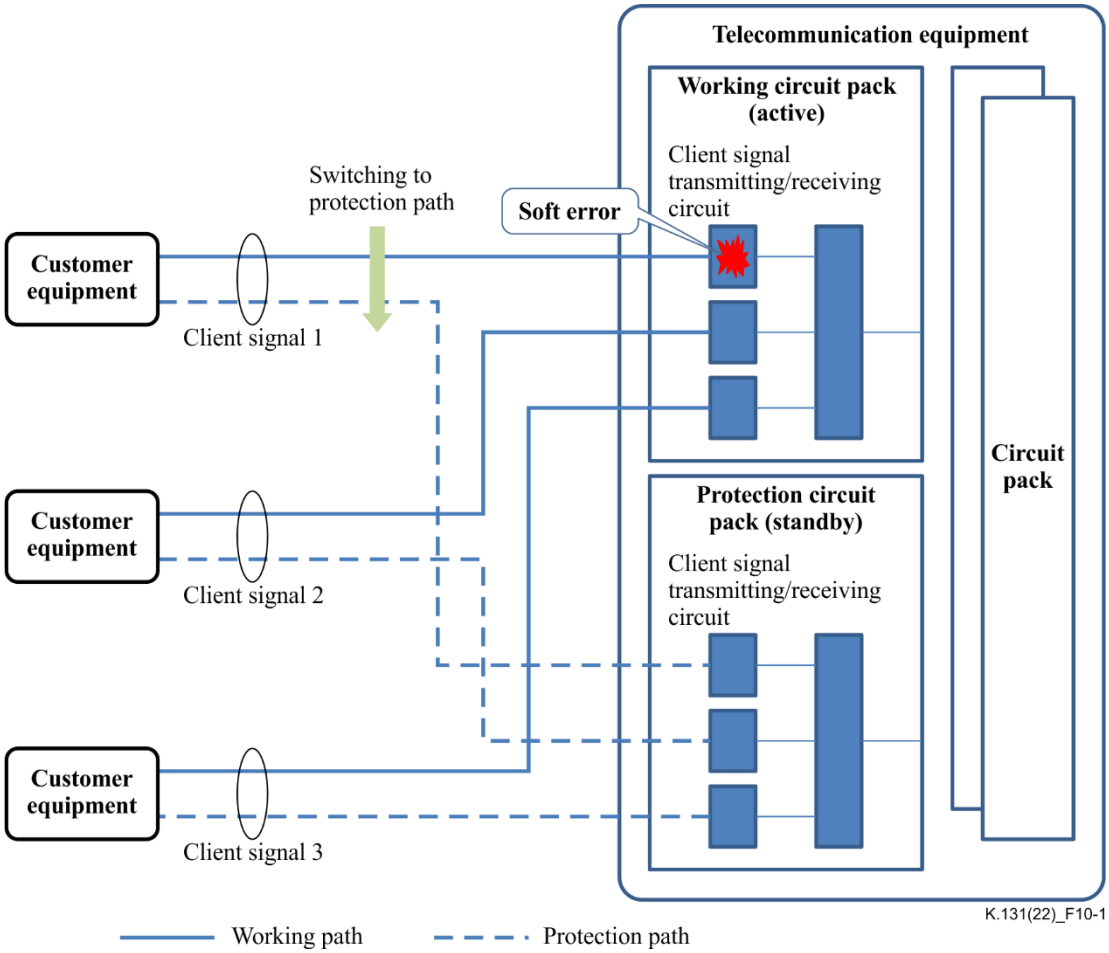

Figure 10-1 – Example of a redundant configuration of circuit packs in equipment

In the case shown in Figure 10-1, it is assumed that the following limitations exist in the execution of countermeasures using redundant configuration.

a) It is possible to switch only the transmitting and receiving circuit block for a client signal between active and standby condition, irrespective of others, when a soft error is detected.

b) It is not possible to reinitialize a specific function block or overwrite its setting data and it is necessary to reinitialize the circuit pack to recover from a soft error.

In Figure 10-1, the working circuit pack and protection circuit pack form a redundant configuration and all working paths of client signals 1 to 3 are processed in the working circuit pack. It is assumed that a soft error occurred in the circuit block for client signal 1, while all client signals 1 to 3 are transmitting through transmitting and receiving circuit blocks in the working circuit pack. Client signal 1 can be restored to normal service condition apart from an instantaneous interruption from the automatic switching to the transmission and reception circuit block in the protection circuit pack according to condition a) in the previous paragraph.

However, it is also necessary to switch client signals 2 and 3 from circuit blocks in the working circuit pack to those in the protection circuit pack because the reinitialization of the working circuit pack is necessary to carry out soft error correction and recovery of the circuit block for client signal 1

according to condition b) in the previous paragraph. During this series of operations, signal interruption may possibly occur at client signals 2 and 3, which have not been affected by the soft error itself.

If the impact of a short interruption of client signals 2 and 3 is significant, it is necessary to select the time to switch the client signals between redundant signal blocks and execute soft error correction, e.g., when the impact of a client signal interruption is permissible. In this case, the timing of the switching should be determined by maintenance personnel in cooperation with customers and operated manually. Therefore, the case should be counted as a failure regarding the MR.

Whether client signal interruption for soft error measures is allowed depends on the requirements of each carrier. Therefore, equipment should be designed to allow carriers to select an application method for soft error measures, i.e., by automatic operation of equipment or by manual operation at the discretion of maintenance personnel.

10.2 Design method of notification message regarding soft error measures

This clause describes recommended methods for sending a notification message to maintenance personnel when soft error measures are implemented.

On-site maintenance work, such as circuit pack replacement, is the primary procedure to recover from physical fault failures. In contrast, it is not necessary to replace circuit packs to recover from a failure state caused by a soft error since the following measures in equipment and actions by maintenance personnel can be undertaken:

– in most cases, automatic recovery processing installed in the equipment is effective and it is not necessary for the maintenance personnel to take action;

– in other cases, recovery processing by maintenance personnel is primarily based on remote control and on-site work is very rare.

Thus, action by maintenance personnel is not always necessary for soft errors, unlike physical fault failures. It is desirable to make it easy to distinguish between normal hardware failure messages and notification messages for countermeasures to rectify soft errors, so as not to initiate unnecessary maintenance work.

The method of transmitting the notification message for a soft error that needs a maintenance personnel response should be different from that when automatic measures are applied. Details of notification messages are given in Annex A.

It is not necessary to issue a notification message when all the following conditions are satisfied:

1) the measures to rectify soft errors are automatically applied;

2) the failure is restored instantaneously without affecting service; and

3) equipment state change such as redundant system switching or reinitialization is not involved.

Even in this situation, it is recommended that the soft error occurrence history be saved in the performance monitor, which maintenance personnel can obtain.

10.3 Saving soft error occurrence history

Notification messages should be issued for maintenance personnel as described in clause 10.2 when soft error measures are executed. Furthermore, it is important to record the equipment status history for failure analysis. Accordingly, the details of the events recognized as soft errors should be saved in an equipment log, including the time at which the event was detected as well as the details of the error, e.g., a parity error, CRAM error or device error. This makes it easier to determine the cause of failures by analysing the records in the log when the circuit pack is returned to the manufacturer for repair. It is recommended that the log be saved for the lifetime of the equipment for future failure cause investigation.

10.4 Soft error measures for initial start-up data storage memory

Data and programs required for start-up of telecommunication equipment are normally stored in non-volatile memory within the equipment as mentioned in clause 6.3.3. If the soft errors in the memory are left unrecovered, multiple equipment failures may occur and replacement circuit packs may run short. If the occurrence of such a failure is not acceptable and it does not satisfy the reliability requirements, automatic restoration of readout data by ECC correction or measures to check data in the memory periodically, and detect and correct errors early should be implemented.

10.5 Identification of physical fault failure to prevent repetition of soft error measures

It is necessary to prevent endless repetition of detection and correction in the case of a physical fault failure, since this erroneous condition continues even after data correction in measures to rectify soft errors. To handle this, it is necessary to install a function to ascertain whether the soft error correction measure has worked effectively by providing an appropriate restoration protection time to help distinguish between a soft error failure and a physical fault failure.

10.6 Notes on use of CPU internal memory

Some general-purpose CPU devices have neither parity nor ECC check functions in internal memory. When internal memory is used as operational work areas for running programs, WDT detection can be applied. However, if it is used for setting data storage memory, soft errors may not be recovered by overwriting and this can lead to operational failure in the equipment. Accordingly, it is not recommended to use internal memory for setting data storage memory in the absence of parity and ECC check functions.

11 Soft error reliability evaluation methods

This clause describes soft error reliability evaluation methods to apply after equipment design.

Table 11-1 shows evaluation methods. These evaluations are to estimate the equipment reliability regarding soft errors with respect to the total operation of the equipment including hardware, control programs, etc. On this basis, the appropriateness of measures and conformity to requirements are analysed. According to the results, if the requirements are not satisfied, it is necessary to redesign the equipment.

Table 11-1 – Soft error reliability evaluation methods

Type		Method	Main use	Reference
Theoretical	Reliability calculation for design of soft error measures	Update Table 8-4 by calculating the failure rate after soft error measures have been implemented	Applied when equipment manufacturers check the validity of countermeasure design	Table 11-2
Actual equipment	Error injection test	Invert arbitrary bit in the device to generate a pseudo soft error during equipment operation		[ITU-T K-Suppl.11]
	Neutron irradiation test	Irradiate the entire equipment with a fast neutron beam from a particle accelerator	Test to confirm conformity to reliability classes	[ITU-T K.130]

The SEFR reflecting the countermeasures incorporated in the circuit design and control program design should be calculated according to the method shown in clause 8.2, corresponding to that calculated at the initial stage of the design. The evaluation should be executed for the issues in Table 11-2.

Table 11-2 – Example of soft error measures design evaluation

Impact on client signal when the function block fails (Figure 6-1)	Type		Functions/usage conditions	Circuit classification	SEFR calculation (FIT)	
					Service reliability requirement	Maintenance reliability requirement
No impact	(1) CPU peripheral circuit	1	Core	Logic circuit	Calculate FIT values after implementation of soft error measures	
		2	Internal memory (operation control, setting data, data buffer)	SRAM		
		3	Main memory (operation control, setting data, data buffer)	DRAM		
		4	Backup memory (setting data)	Flash memory		
		5	Cache memory (operation control)	SRAM		
	(2) FPGA peripheral circuit	1	External memory (setting data)	Flash memory		
Impact		2	Core	Logic circuit		
		3	Configuration memory (setting data)	SRAM		
		4	Block memory (operation control, setting data, data buffer)	SRAM		
		5	External memory (data buffer)	SRAM		
		6	External memory (setting data)	SRAM		
	(3) ASIC peripheral circuit	1	Core	Logic circuit		
		2	Internal memory (operation control, setting data, data buffer)	SRAM		
		3	External memory (data buffer)	SRAM		
		4	External memory (setting data)	SRAM		

Reliability evaluation methods for actual equipment include the error injection test and neutron irradiation test. The error injection test reverses the value of arbitrary bits in the equipment memory during operation to generate soft errors artificially. This method makes it possible to verify the operation of the soft error measures in the equipment. In particular, the error injection tool provided by the FPGA vendor can be used for CRAM of FPGA, which is susceptible to soft errors. The neutron irradiation test uses an accelerator-driven neutron source to irradiate neutrons targeting the equipment in operation at a rate several million times that found in the actual environment. The influence of soft errors can be evaluated under the same equipment configuration and operating conditions as the actual ones by the irradiation test.

Design evaluation by calculation for soft error measures and the error injection test are mainly applied when manufacturers conduct design validity checks. On the other hand, the neutron irradiation test can be used to check conformity to the reliability requirement and the test result is a common measure to guide manufacturers and carriers.

Annex A

Design method for notification message for soft error measures

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

This annex gives details of the concept for designing the notification message for soft error measures described in clause 10.2.

A.1 Notification message on execution of automatic restoration from soft error

Figure A.1 shows a design example for a transmission method for a notification message when restoration from a soft error is automatically executed in the equipment.

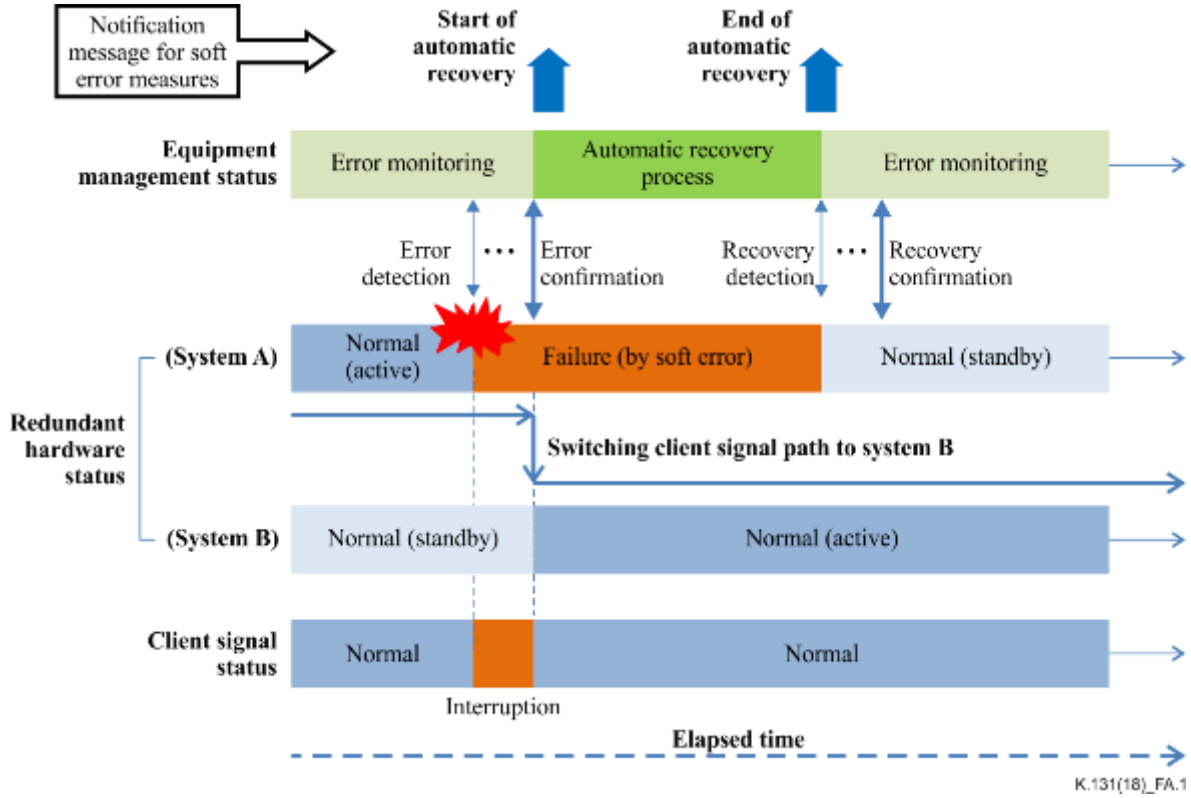

Figure A.1 – Transmission method for notification messages when automatic soft error measures are executed

Figure A.1 shows the changes in the client signal state, the hardware state of the circuit blocks that transfer client signals in system A and system B in a redundant configuration, the equipment management state of the control program and the notification message relating to soft error measures, relative to the elapsed time from left to right.

Assume that a soft error occurs in system A which is active; when the hardware in system A becomes abnormal, this is detected by the control function block and the failure state is determined after a certain time threshold. The client signal state then instantaneously returns to normal by switching the operation from system A to system B.

When soft error measures are not implemented, the notification message is generally sent at this time as an equipment failure alarm to notify maintenance personnel to restore the hardware in system A. However, when soft error measures are implemented, the equipment failure alarm should not be sent, to avoid unnecessary restoration efforts by maintenance personnel.

Instead, system A shall be switched to an inactive state and soft error correction measures as in clause 9.3 shall then be applied automatically to system A. In order to report that automatic restoration has started and completed in the equipment, a notification message for these events should be sent at both times. After that, the management system checks the hardware state to confirm the equipment has recovered after a certain time. The pair of notification messages should be assigned a notice level because they signify a need to analyse the soft error occurrence history and do not require handling by maintenance personnel. Figure A.1 shows an example when a soft error affected the client signal, but the same notification type should be sent when redundant system switching for recovery occurs, even if the soft error had no impact on the client signal.

On the other hand, failures due to a soft error and a physical fault cannot be distinguished at the time hardware fails. Figure A.2 shows an example of a notification transmission method when the equipment automatically starts the restoration procedure for soft errors if failure is caused by a physical fault.

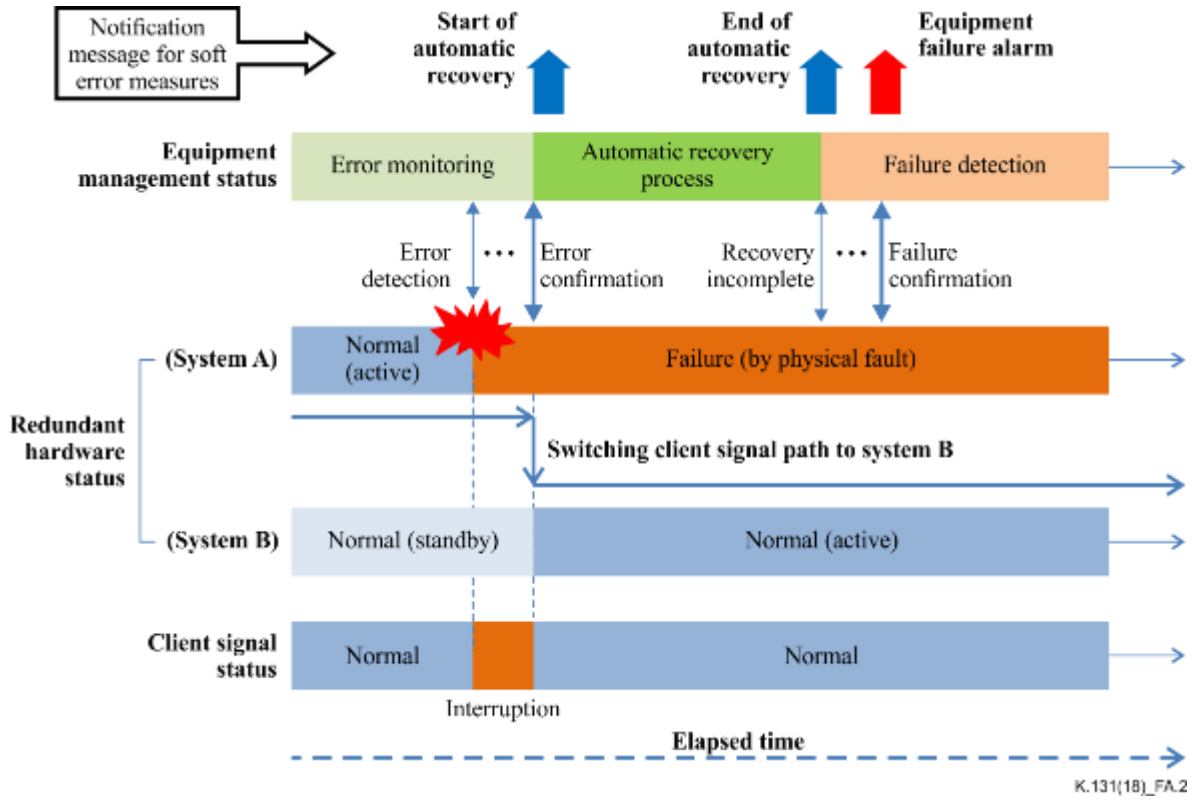

Figure A.2 – Transmission method for notification messages on automatic soft error measures by equipment to rectify physical fault failure

This follows the same sequence as in Figure A.1 until the end of the restoration procedures, which means notification messages for the start and end of the automatic soft error recovery process are sent. However, in the event of a physical fault failure, the failure is not fixed, and the failure state continues after the end of the recovery process. In this case, an equipment failure alarm message should be sent when the failure is discovered to persist because the maintenance personnel must be notified to carry out hardware restoration such as circuit pack replacement. From the viewpoint of improvement of system reliability and reduction in the workload of maintenance personnel, restoration procedures to rectify possible soft error failures should be applied prior to the physical fault restoration, but the equipment failure alarm shall be sent out when the failure cannot be fixed automatically.

A.2 Notification message on execution of manual restoration from soft error

Figure A.3 shows a design example of a transmission method for a notification message if restoration from a soft error needs to be executed by maintenance personnel. This example shows a case where a soft error occurs in a transmitting and receiving circuit block for client signal 1 in Figure 10.1. The working circuit pack and protection circuit pack form a redundant configuration and all working paths of client signals 1 to 3 are processed in the former. Assumptions a) and b) in clause 10.1 apply in this case.

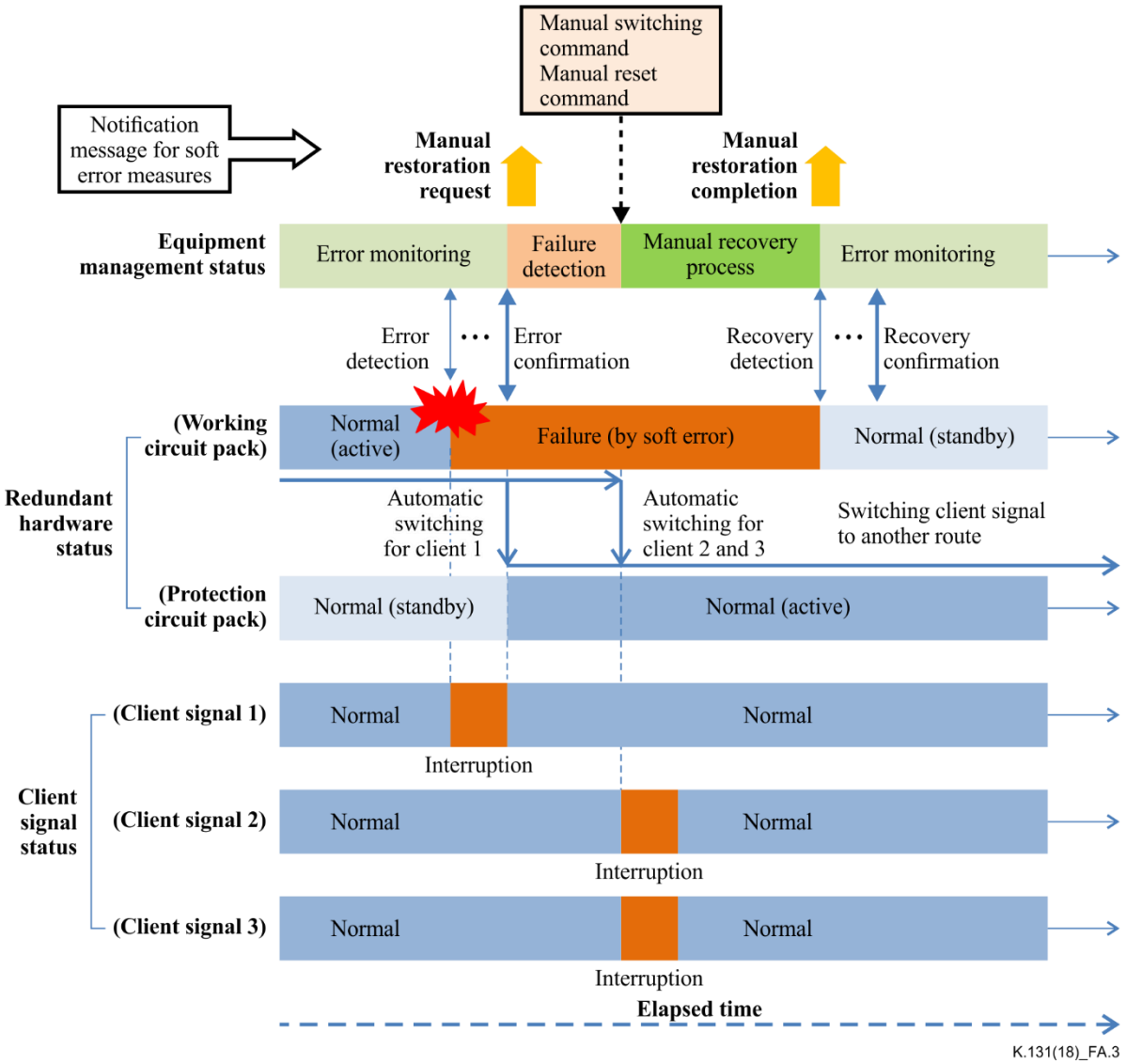

Figure A.3 – Transmission method for notification messages on manual soft error measures by maintenance personnel

When a soft error occurs in the transmitting and receiving circuit for client signal 1 and failure is determined, the signal path for client signal 1 is switched to the circuit block in the protection circuit pack. As a result, client signal 1 recovers the service even if it is briefly interrupted.

Client signals 2 and 3 through the working circuit pack are interrupted if a soft error measure, such as signal path change and reinitialization of the circuit pack, is executed in the working circuit pack and manual operation of maintenance personnel is necessary as described in clause 10.1. Therefore, in this case a request message for a manual restoration operation should be sent. In response to this, maintenance personnel switch the signal paths for client signals 2 and 3 to the circuit blocks in the protection circuit pack when the impact on service is permissible and then stops service of the working

circuit pack. Thereafter, maintenance personnel restore the working circuit pack by resetting it by remote control.

Next, a notification message is sent when the recovery process for soft error measures is completed. After that, it is confirmed whether equipment has recovered after a specified elapsed time.

Thus, the equipment can be used continuously as it is and it is not necessary to replace a circuit pack since the maintenance personnel can recognize from the notification message that it is a failure caused by a soft error and has recovered normally. The notification messages for request and completion of manual restoration should be at an alarm level similar to equipment failure alarms to notify the maintenance personnel that action is required.

Figure A.4 shows an example where the restoration process in Figure A.3 is carried out and eventually it is found to be a physical fault failure.

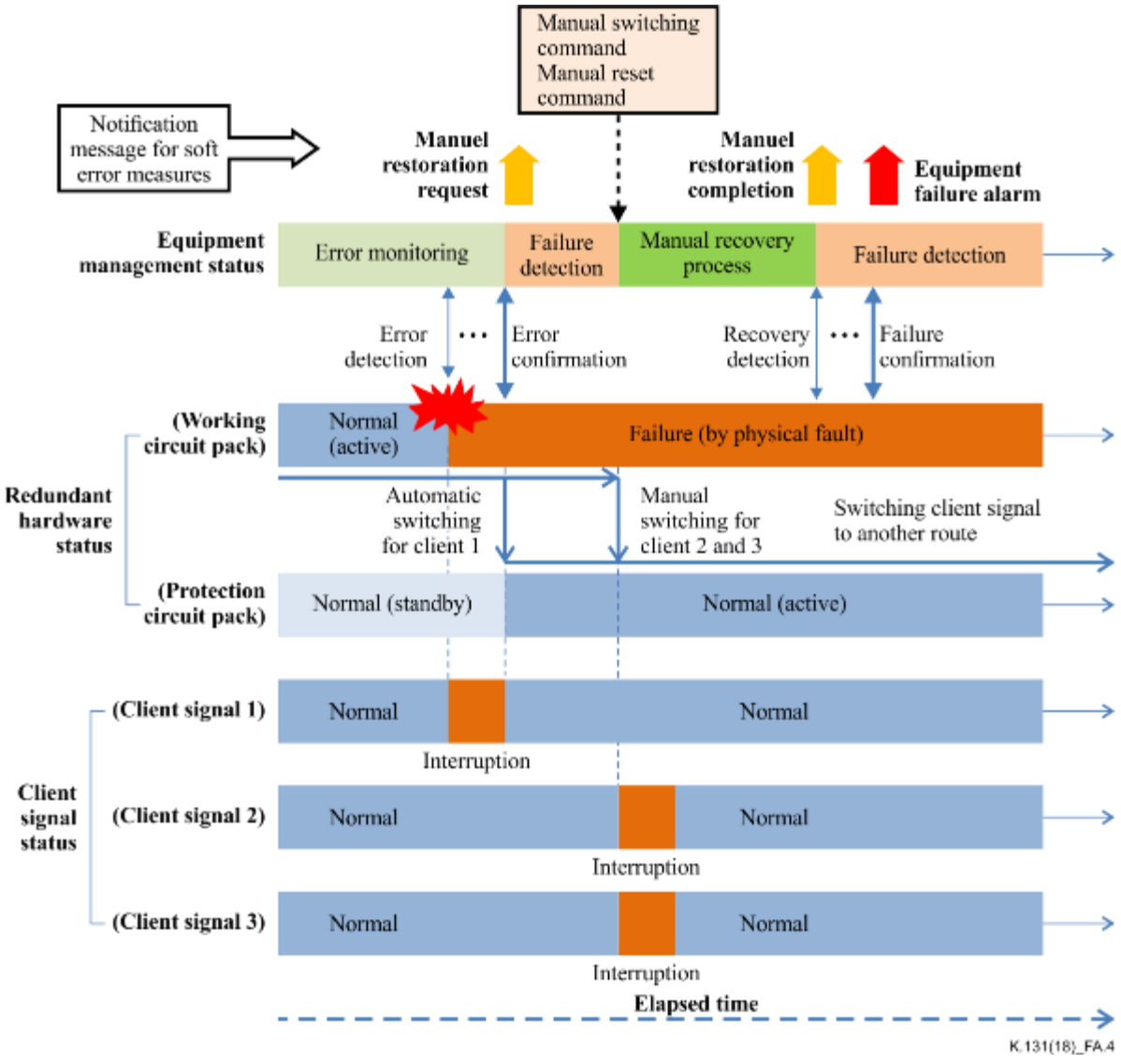

Figure A.4 – Transmission method for notification messages on manual soft error measures by maintenance personnel to rectify physical fault failure

Figure A.4 follows the same sequence as Figure A.3 until the soft error manual recovery process is completed and its notification message is sent. However, in the event of a physical fault failure, the failure is not fixed, and the failure state continues after the end of the recovery process. In this case, an equipment failure alarm message should be sent when the failure is discovered to persist because

maintenance personnel must be notified to carry out hardware restoration such as a circuit pack replacement. From the viewpoint of improving system reliability and reducing the workload of maintenance personnel, restoration procedures to rectify a possible soft error failure should be applied prior to the physical fault restoration, but the equipment failure alarm shall be sent out when the failure cannot be fixed by the soft error measures.

Appendix I

Trends in semiconductor device soft error tolerances

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

Static random access memory

In the semiconductor industry, it is well known that SRAM is the type of device most vulnerable to soft errors among circuit elements such as logic circuits, DRAM, SRAM and flash memory. Progress in the scaling of LSI processes for semiconductor devices tends to increase the SER. Almost all soft errors occur in SRAM devices in the field.

In the case of soft errors in SRAM, not only a single SRAM cell upset, but also the upset of multiple adjacent SRAM cells should be considered. If an upset occurs, the correct values must be rewritten because the upset values are being stored. Recent systems using SRAM devices have adopted several measures such as ECC generation, interleaving and periodic validation of stored data.

Dynamic random access memory

Around 1980, soft errors that occurred in DRAM cell capacitors were problematic. The major cause of DRAM soft errors is alpha particles emitted from trace nuclear impurities such as the uranium in an LSI package. Several measures have been adopted, such as using low alpha particle-emitting package materials that have reduced contents of radioactive impurities including ^{238}U and ^{232}Th. In addition, the change in structure of DRAM cell capacitors, from planar to stacked or substrate-type trench, has resulted in great improvement in the SER. As a result, SER per memory capacity of DRAM is 10^{-3} to 10^{-4} times that of SRAM. However, during equipment design, it is necessary to calculate the actual SER corresponding to the used capacity and consider the necessity for measures.

Flash memory

It was thought that soft errors did not occur in flash memory. In the case of the predominant floating-gate systems, data are stored in the array of flash memory cells by storing an electric charge (electrons) on an electrode surrounded by insulators. Corruption of the data stored in flash memory cells is thought not to occur even if the charged particles enter the flash memory cell. However, recent research has revealed that soft errors can occur in flash memory cells because progress in scaling has decreased the number of stored electrons. The SER of flash memory has increased because both NOR- and NAND-type flash memory cells have been miniaturized with greater capacity and their structures have been changed from SLC to MLC and from MLC to TLC. However, an experimental result shows that the SER per memory capacity in flash memory is about 1% of the SER of SRAM. In an experimental measurement, the cross-section of neutron-induced soft errors of the MLC flash memory fabricated in the 25 nm process was shown to be of the order of 10^{-14}, which is comparable with that of SRAM from the viewpoint of these measures [b-Bagatin]. Therefore, at the time of equipment design, it is necessary to calculate the actual SER corresponding to the used capacity and consider the necessity of measures.

Logic circuits

Previously, soft errors were problematic in the application of semiconductor memory. SRAM used as the cache memory of a microprocessor is usually able to tolerate soft errors by using techniques such as parity check and ECC check. Around 2009, soft errors occurring in the large logics, or logic circuits, gained prominent attention as the semiconductor manufacturing process was miniaturized. Unlike memory devices, the ECC check technique cannot be applied to logic circuits. Thus, there has been a lot of active research on topics relating to the soft error tolerance of logic circuits.

Logic circuits can be categorized into sequential circuits and combinational circuits. A sequential circuit determines its outputs according to the inputs and stored internal states. Typical sequential

circuits are the flip-flop, latch and counter. In contrast, a combinational logic determines its output according to its inputs only. Typical combinational circuits include the inverter, the NOR gate and the NAND gate. There is a vast difference in the soft error resilience between a sequential circuit and a combinational circuit. Charged particles generated by neutron collisions striking the sequential circuit can easily upset the stored values within the circuit. For example, the SER of the combinational circuit fabricated in a 32 nm CMOS process is reported to be less than 10% of the rate of the sequential circuit [b-Gadlage]. Thus, the main measures for logic circuits are the same as the measures for sequential circuits.

However, recent research reports have shown that soft errors in combinational circuits can be problematic, particularly in the case of high-speed processors. This is why the number of latches of the calculated values increases as the clock frequency increases and the rate of incorrect latching values that are upset by ion strikes increases [b-Gill]. Currently, low-cost measures to prevent this type of error have not been found and fast and accurate analytical techniques for lowering SERs are required. Estimation techniques have been proposed for soft error vulnerability.

As previously described, the number of soft errors in logic circuits is expected to be considerable as a result of miniaturization of the semiconductor manufacturing process and the growth in semiconductor device density. For example, applying a redundant circuit is the most reliable measure to rectify soft errors, but this has the drawback of an increase in the silicon area. Research on measures suitable for practical use is still being conducted. The trend should be kept as a focus, although soft errors in logic circuits have not appeared to be problematic in field tests and neutron irradiation tests using a particle accelerator.

Bibliography

[b-ITU-T K-Suppl.11] ITU-T K-series Recommendations – Supplement 11 (2018), *ITU-T K.131 – Soft error measures of field programmable gate arrays*.

[b-Bagatin] Bagatin, M., Gerardin, S., Paccagnella, A., Ferlet-Cavrois, V., Visconti, A., Gorini, G., Andreani, C., Frost, C.D. (2013). Neutron and alpha SER in advanced NAND flash memories. In: *14th European Conference on Radiation and Its Effects on Components and Systems (RADECS)*, H-3, pp. 1-4. New York, NY: IEEE.

[b-Gadlage] Gadlage, M.J., Eaton, P.H., Benedetto, J.M., Turflinger, T.L. (2005). Comparison of heavy ion and proton induced combinatorial and sequential logic error rates in a deep submicron process. *IEEE Trans. Nucl. Sci*. **52**(6), pp. 2120-2124.

[b-Gill] Gill, B., Seifert, N., Zia, V. (2009). Comparison of alpha-particle and neutron-induced combinational and sequential logic error rates at the 32 nm technology node. In: *2009 IEEE International Reliability Physics Symposium*, pp. 199-205. New York, NY: IEEE.

[b-Iwashita] Iwashita, H., Funatsu, G., Sato, H., Kamiyama, T., Furusaka, M., Wender, S.A. Pitcher, E., Kiyanagi, Y. (2020). Energy-resolved soft-error rate measurements for 1-800 MeV neutrons by the time-of-flight technique at LANSCE. *IEEE Trans. Nucl. Sci*. **67**(11), pp. 2363-2369.

[b-Xilinx] Xilinx (2013–21). *Device reliability report – First half 2021 – UG116* (v10.15). San Jose, CA: Xilinx. 93 pp. Available [viewed 2022-02-14] at: https://www.xilinx.com/support/documentation/user_guides/ug116.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022