SUBJECT: SPIRE Failure Detection Isolation and Recovery

PREPARED BY: K.J. King

DOCUMENT No: SPIRE-RAL-PRJ-001978

ISSUE: Issue 1.0 **Date:** 13th July 2004

APPROVED BY:

Instrument Engineer
(B.Swinyard)

AGREED BY:

OPS Scientist
(S. Sidher)

Distribution

B.Swinyard	RAL
Sunil Sidher	RAL
S. Molinari	IFSI
R. Orfei	IFSI
J. Long	RAL

Change Record

ISSUE	DATE	Changes
1.0 Draft 1	17th March 2004	First draft for internal discussion
1.0 Draft 2	16th June 2004	Updated draft for internal review
1.0	13th July 2004	First Version

TABLE OF CONTENTS

FIGURES

TABLES

Glossary

OBS	On-Board Software
SPIRE	Spectral and Photometric Imaging REceiver

1. INTRODUCTION

1.1 Scope

This document defines the requirements on the SPIRE instrument for detection, isolation and recovery from hardware and software failures of the instrument based on the policy described in AD03. The failures to be dealt with are described in AD01 and AD02.

These requirements will lead to requirements on the OBS autonomy function to detect and isolate the failure and provide a mechanism for recovery from it. The implementation of the recovery procedures will be made in the OBS itself and/or in recovery procedures defined for the CDMS.

In this document FDIR actions are described in flowchart form. Actions carried out by the OBS in internal code are labelled 'OBS' and those carried out by the Autonomy Virtual Machine are labelled 'VM'. Actions carried out by the CDMS are labelled 'S/C'.

1.2 Assumptions

1. 'Inhibit TC Execution' implies that the instrument will no longer execute any telecommands received. It will, however, respond with a telecommand reception acknowledgement. This is to stop any newly received TC restarting a VM or sending a command to a subsystem while the recovery is in progress.
2. 'Inhibit Subsystem Commands' implies that all telecommands received by the OBS which would generate commands to a subsystem are inhibited. The OBS is still able to send commands to the subsystem as part of the recovery procedure.
3. The FDIR is suspended on the first instance of an anomaly being detected. I.e. the Autonomy Virtual Machine cannot be interrupted by another error.

1.3 Structure of Document

The failures themselves can be split into two types: those detected by the instrument OBS and handled by it (possibly with help by the S/C CDMS) – these are described in Section2 (subsystem failures), Section 3 (interface failures), and Section 4 (OBS runtime errors); and those detected by the S/C CDMS and dealt with by it – these are described in section 5.

Section 6 contains those general purpose procedures called during some of the recovery actions described in previous sections

1.4 Documents

1.4.1 Applicable Documents

AD01 Hardware Software Interaction Analysis for SPIRE in-flight Autonomy Functions Specification (SPIRE-RAL-NOT-001719), Issue 1.1, 3rd December 2003

AD02 System Operation and FDIR Requirements (H-P-1-ASP-SP-0209), October 2003
Appendix 1: 1553 Bus FDIR

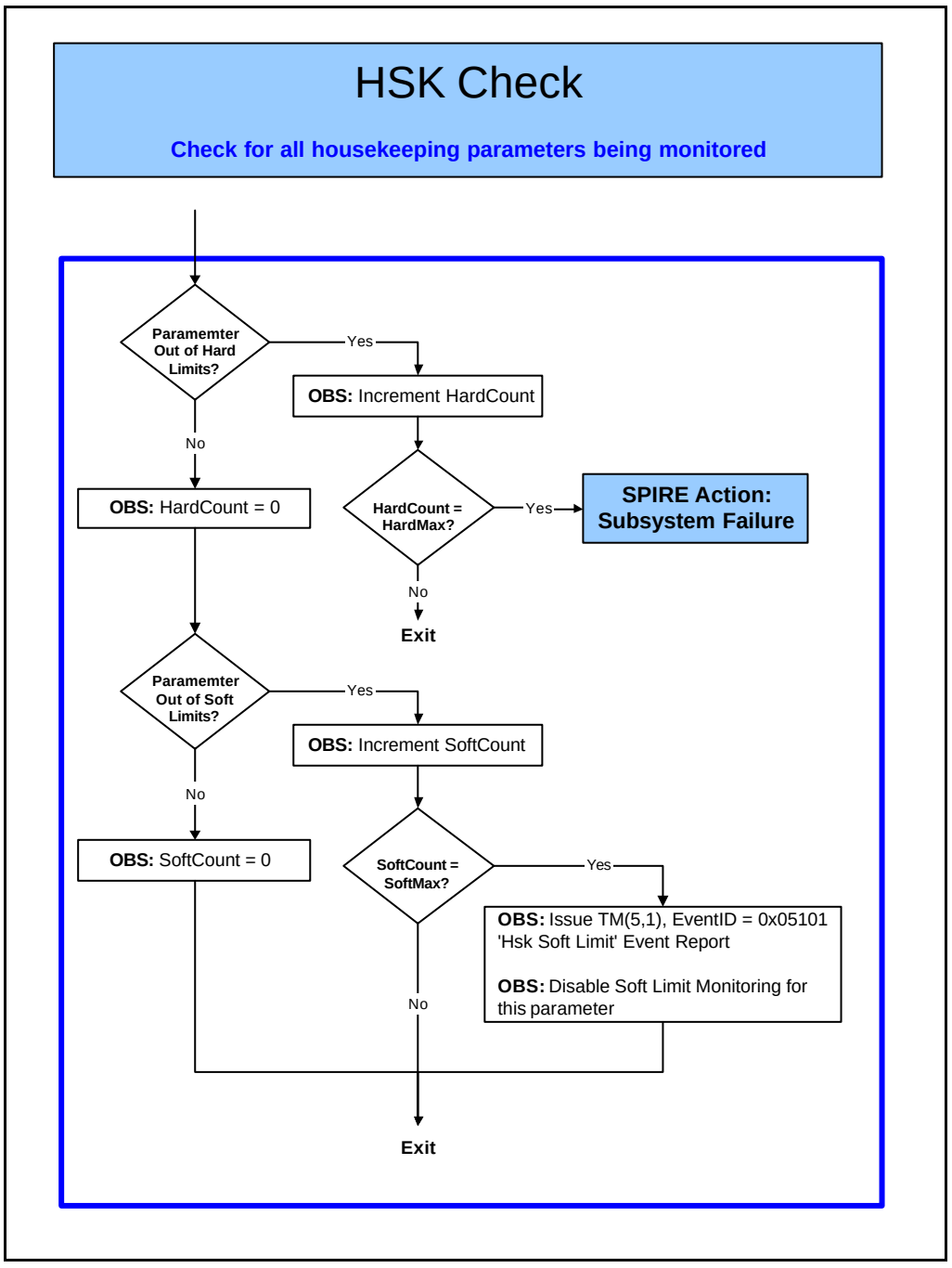
AD03 Failure Detection Isolation and Recovery Policy in the SPIRE Instrument (S{PIRE-RAL-PRJ-001128)

1.4.2 Reference Documents

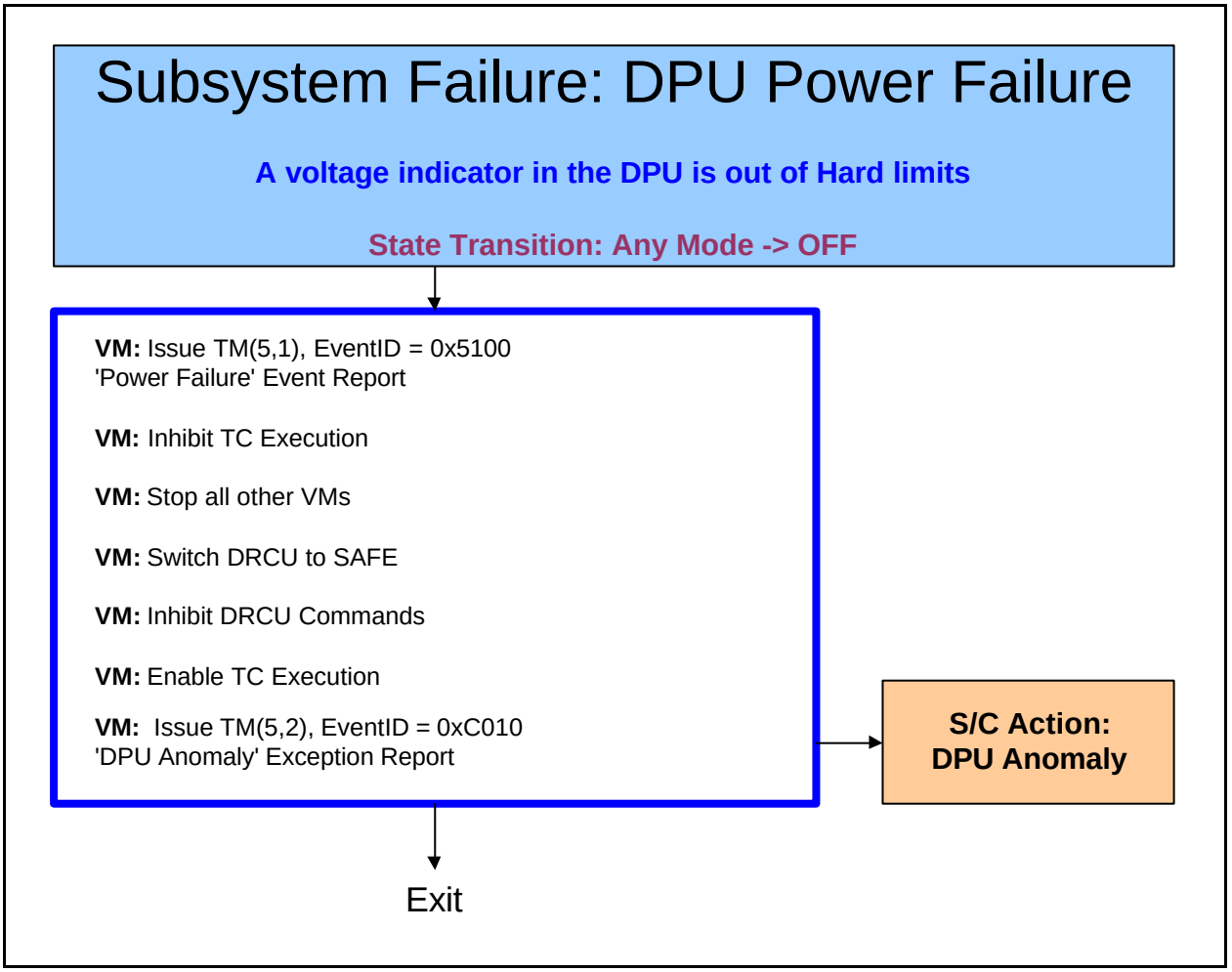
2. SUBSYSTEM FAILURES

Failures within the subsystems of the instrument (both DPU and DRCU) may be identified by monitoring housekeeping parameters generated by the subsystem. Each housekeeping parameter being monitored is checked against a set of soft and hard limits. The parameter has to remain out of limits for a set number (SoftMax or HardMax) of readings before an anomaly is declared. A the soft limit monitoring is disabled once reported, to prevent multiple event packets being generated from a 'noisy' signal. It is expected that it will be re-enabled at the start of each observation, or other suitable time period.

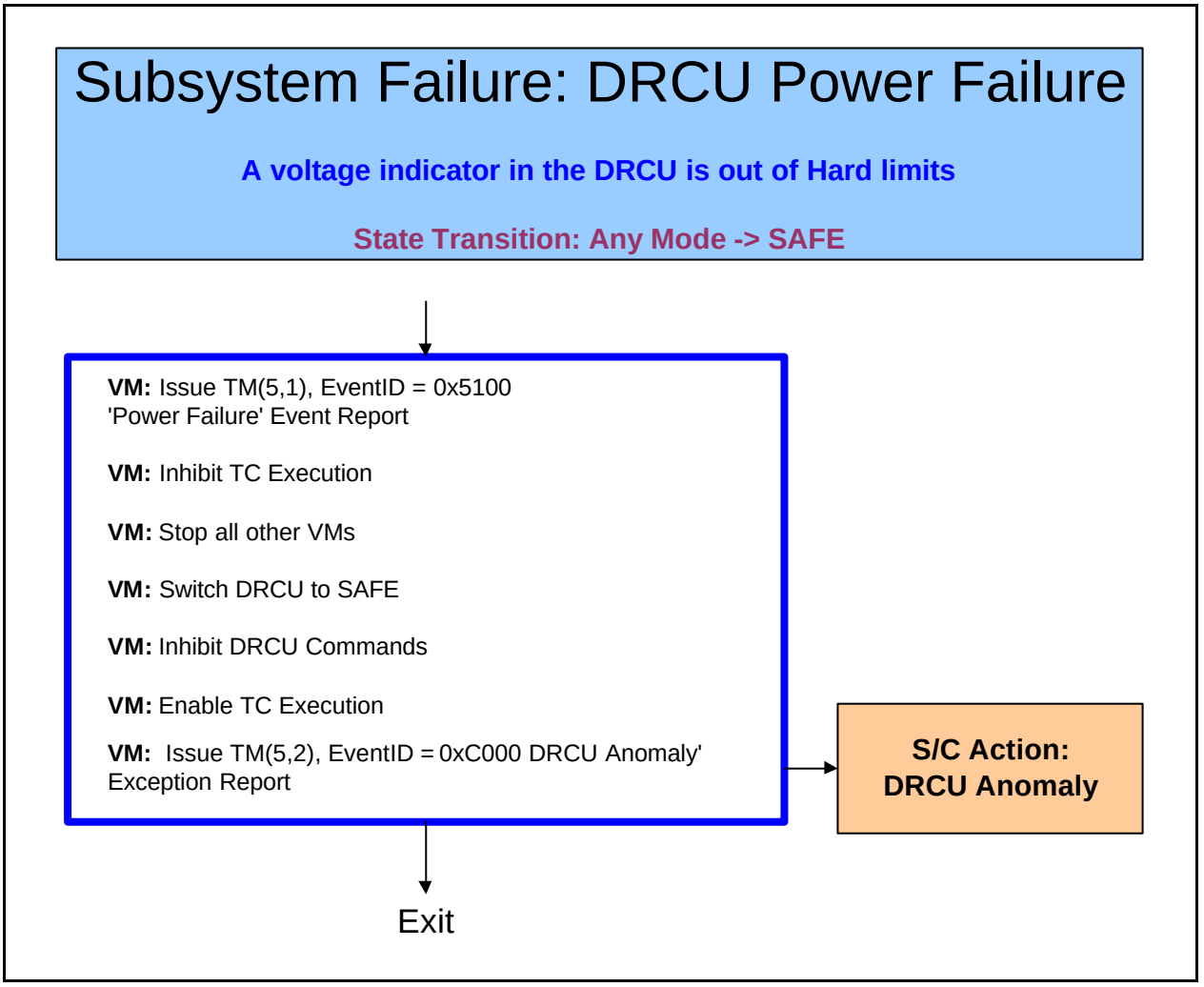
SoftMax and HardMax are set to zero on initialisation of the parameter monitoring system



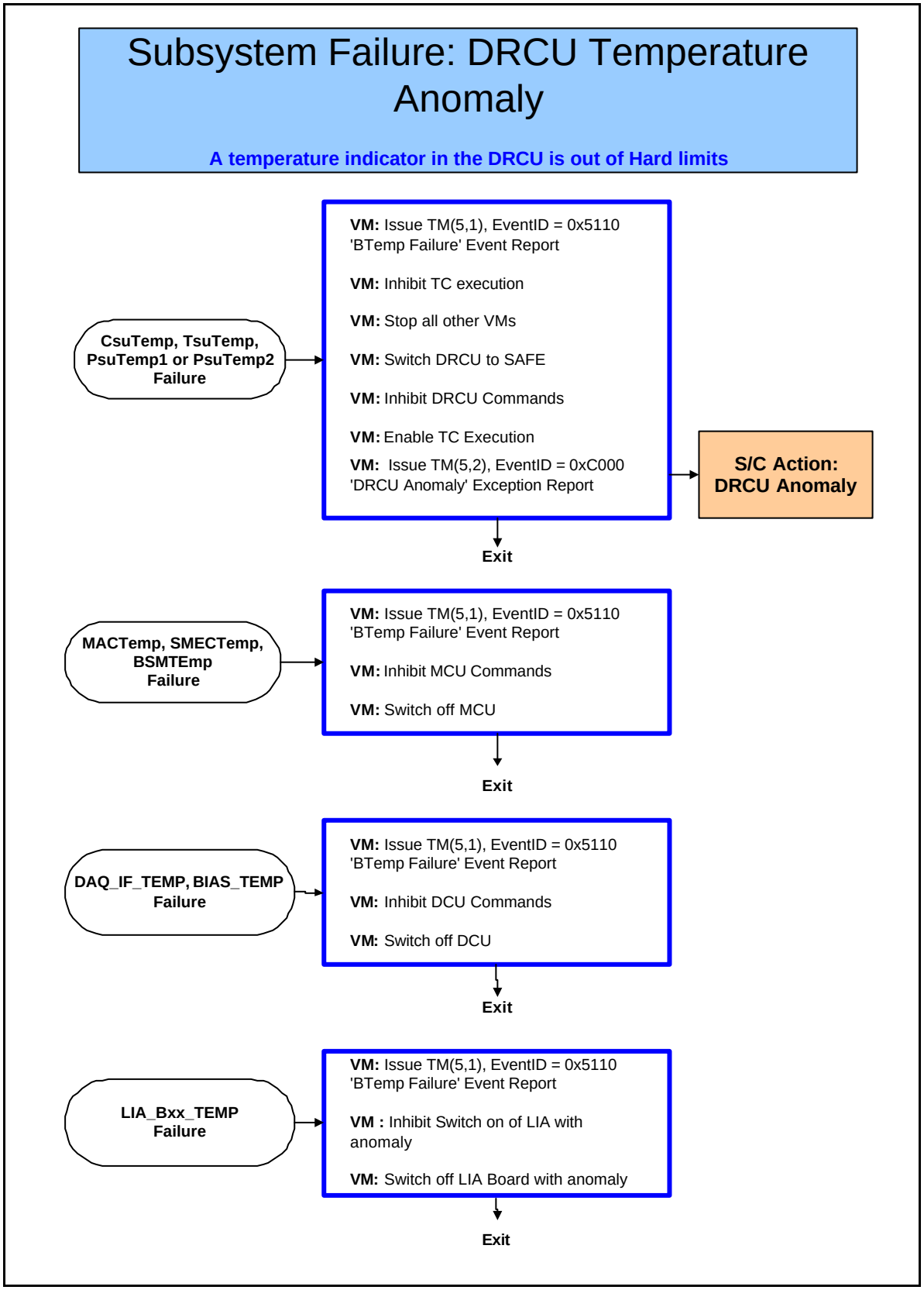
2.1 DPU Power


Subsystem Failure: DPU Power Failure
A voltage indicator in the DPU is out of Hard limits
State Transition: Any Mode -> OFF
VM: Issue TM(5,1), EventID = 0x5100 'Power Failure' Event Report
VM: Inhibit TC Execution
VM: Stop all other VMs
VM: Switch DRCU to SAFE
VM: Inhibit DRCU Commands
VM: Enable TC Execution
VM: Issue TM(5,2), EventID = 0xC010 'DPU Anomaly' Exception Report
S/C Action: DPU Anomaly
Exit

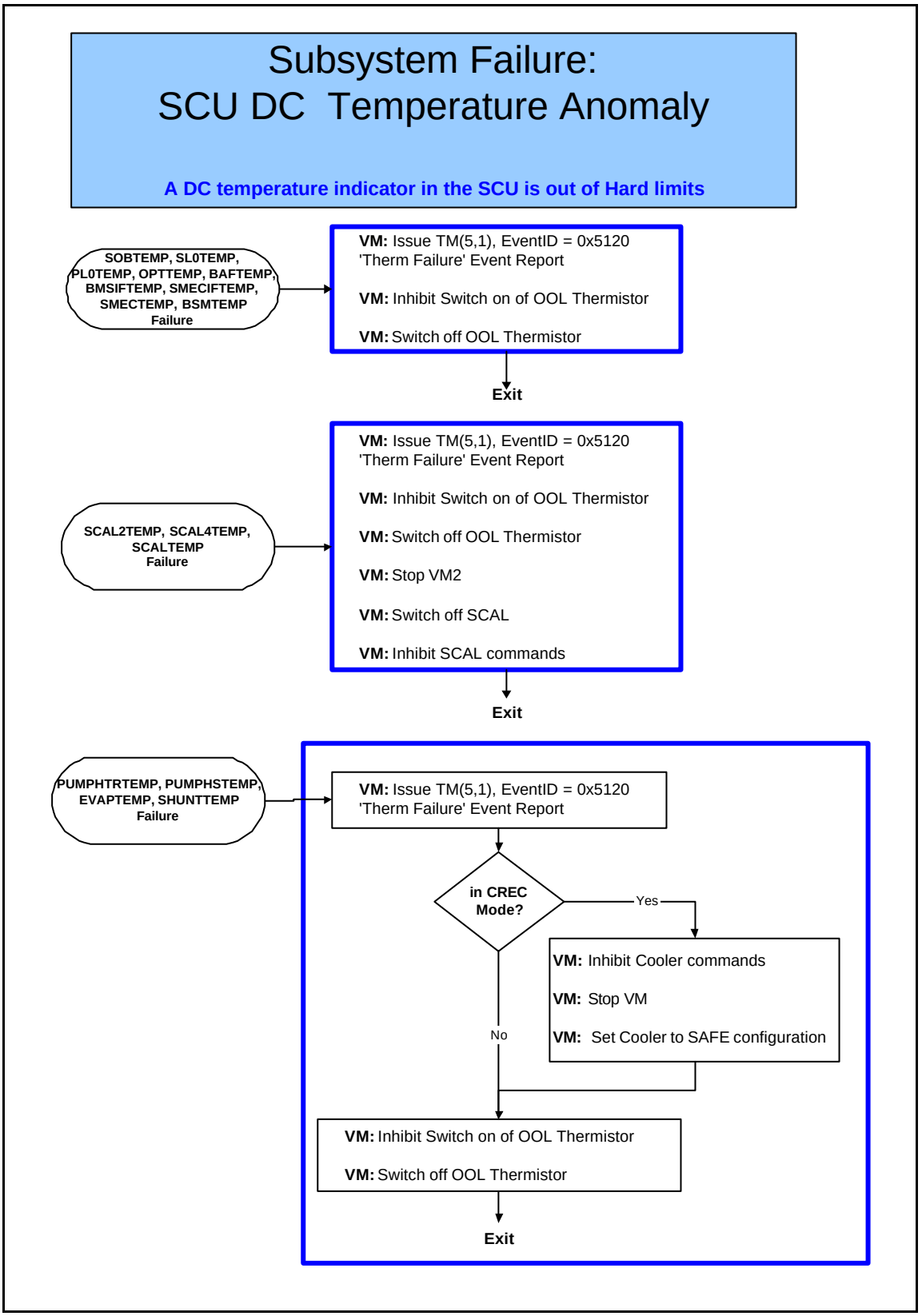
2.2 DRCU Power



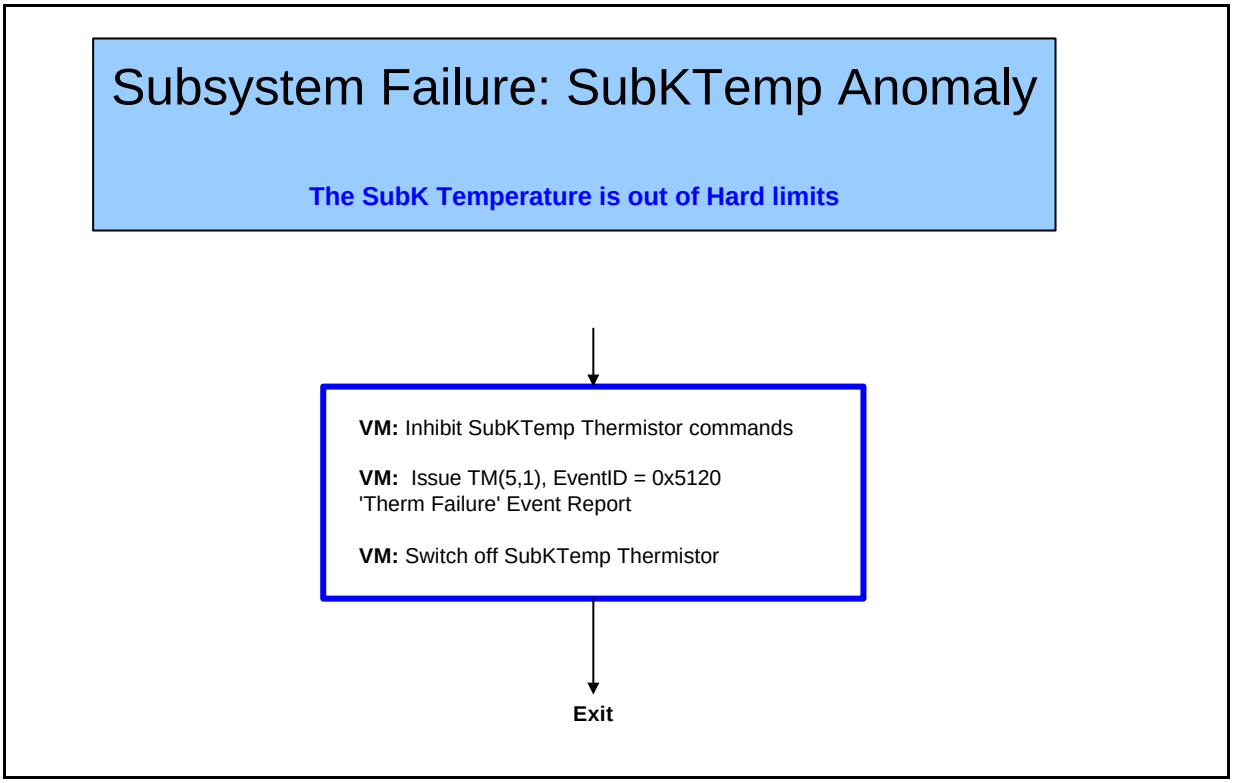
2.3 DRCU Board Temperatures



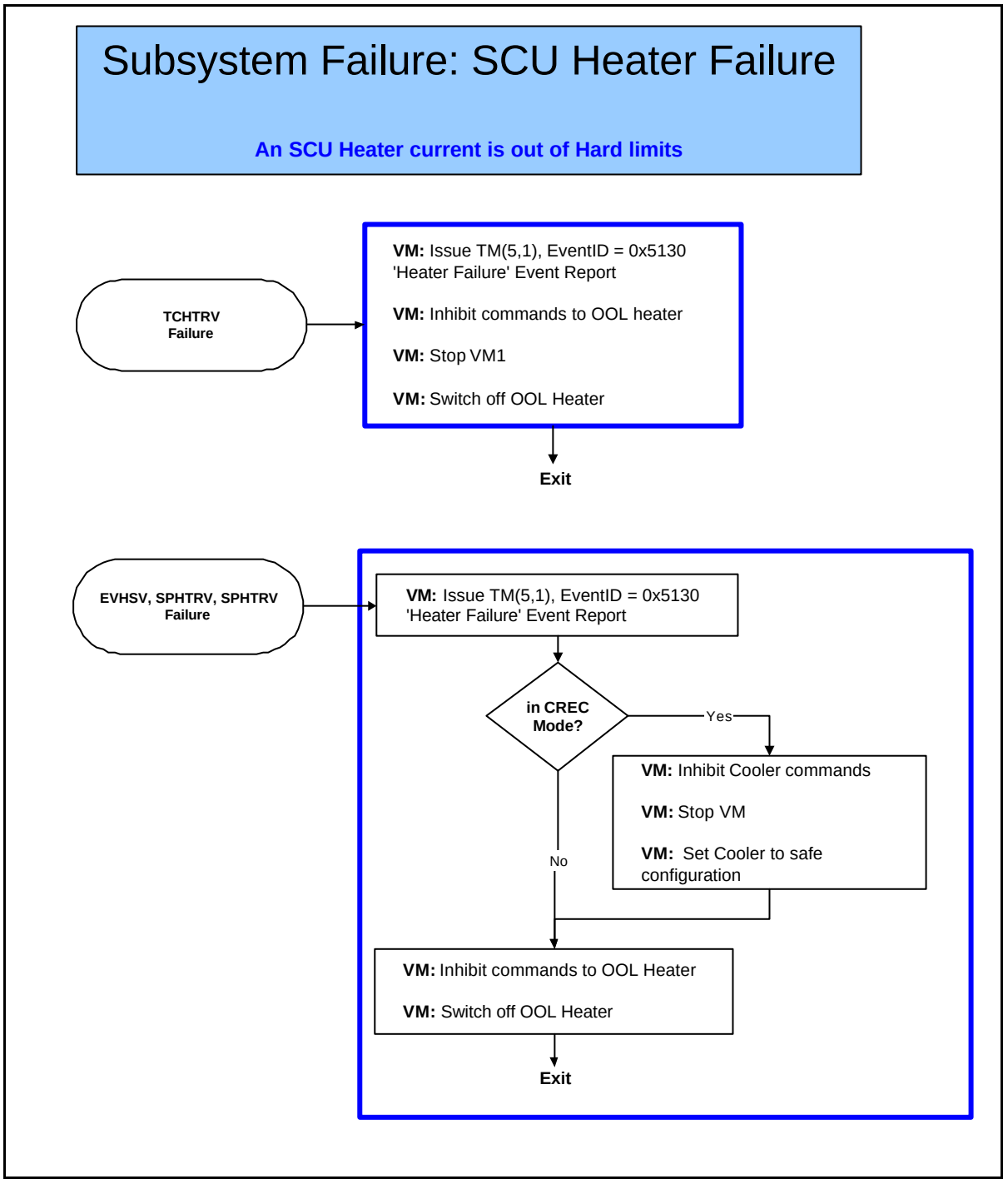
2.4 DC Thermistors



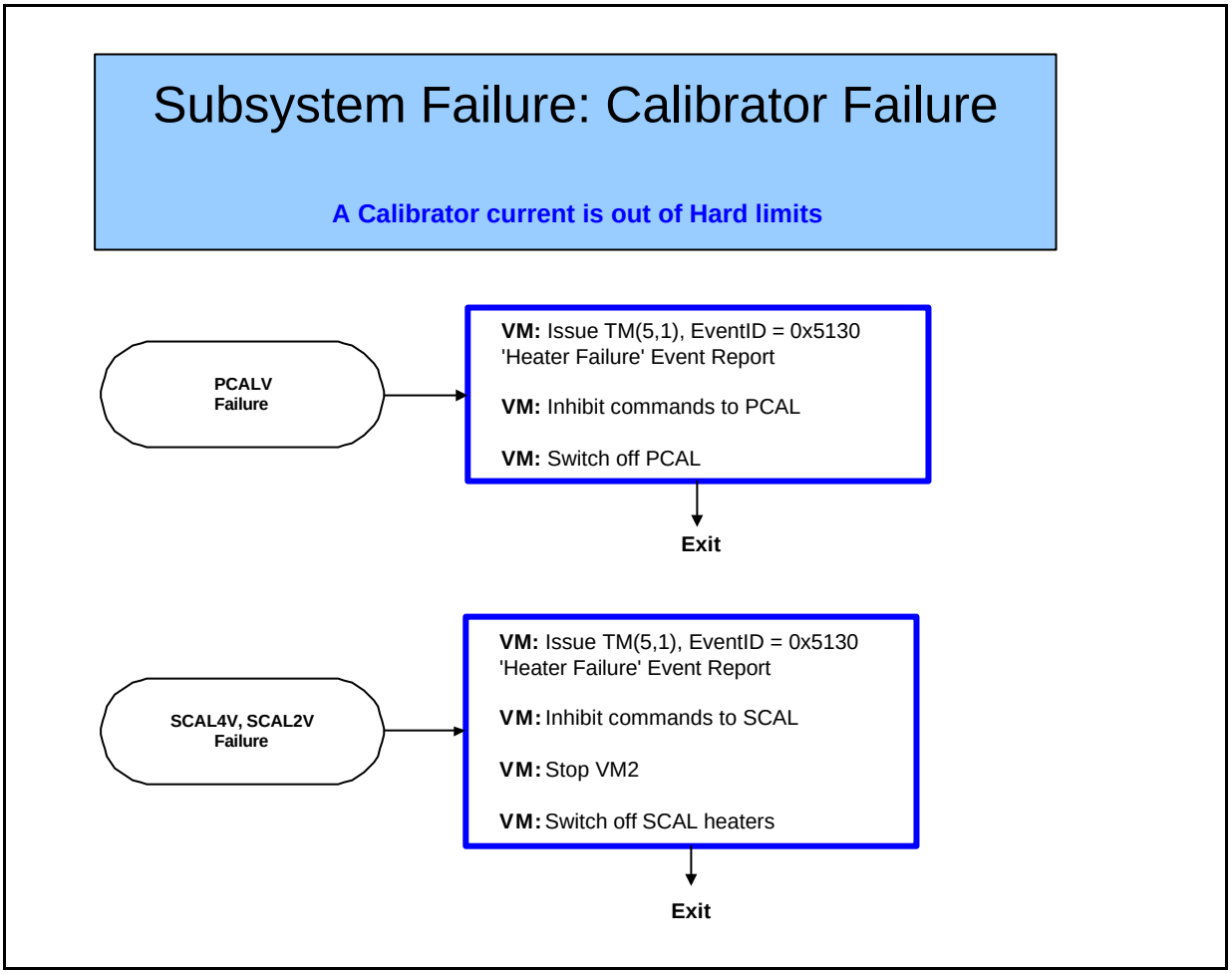
2.5 AC Thermistor



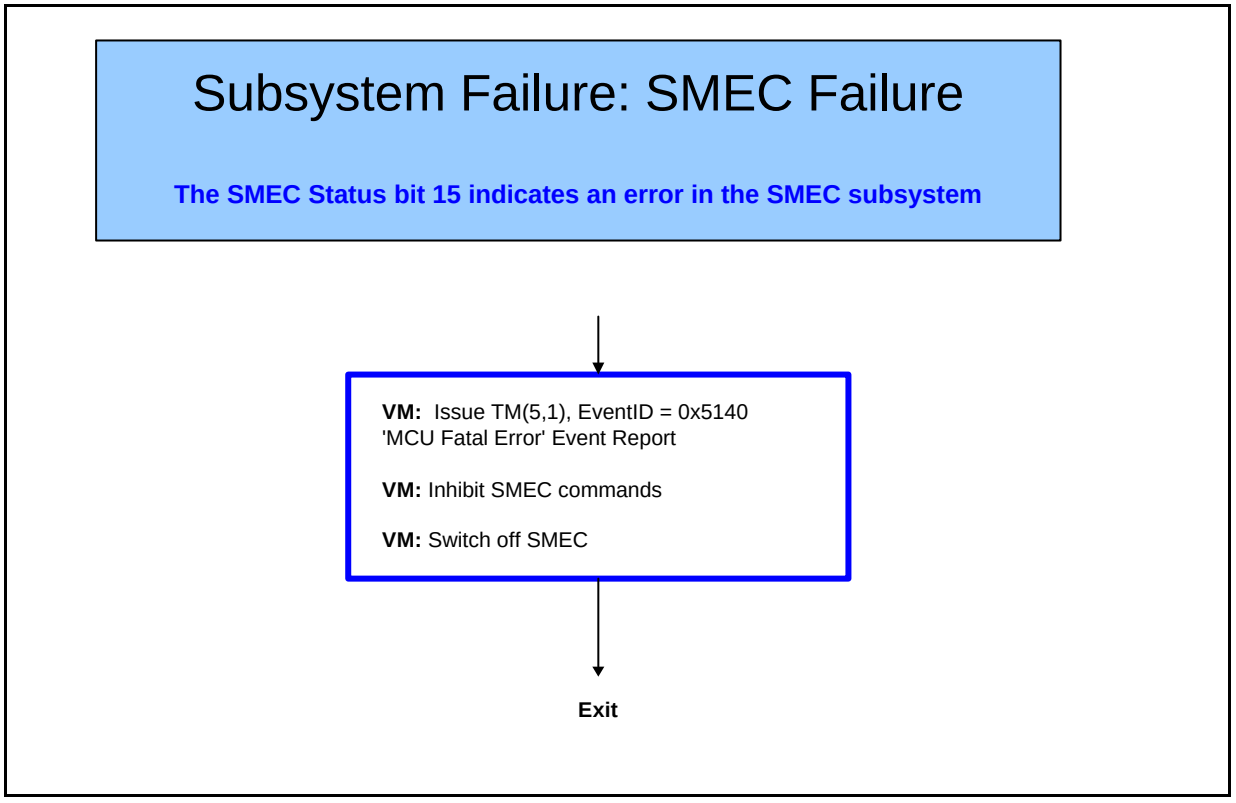
2.6 Heaters


Subsystem Failure: SCU Heater Failure
An SCU Heater current is out of Hard limits
TCHTRV Failure
VM: Issue TM(5,1), EventID = 0x5130 'Heater Failure' Event Report
VM: Inhibit commands to OOL heater
VM: Stop VM1
VM: Switch off OOL Heater
Exit
EVHSV, SPHTRV, SPHTRV Failure
VM: Issue TM(5,1), EventID = 0x5130 'Heater Failure' Event Report
in CREC Mode?
Yes
VM: Inhibit Cooler commands
VM: Stop VM
VM: Set Cooler to safe configuration
No
VM: Inhibit commands to OOL Heater
VM: Switch off OOL Heater
Exit

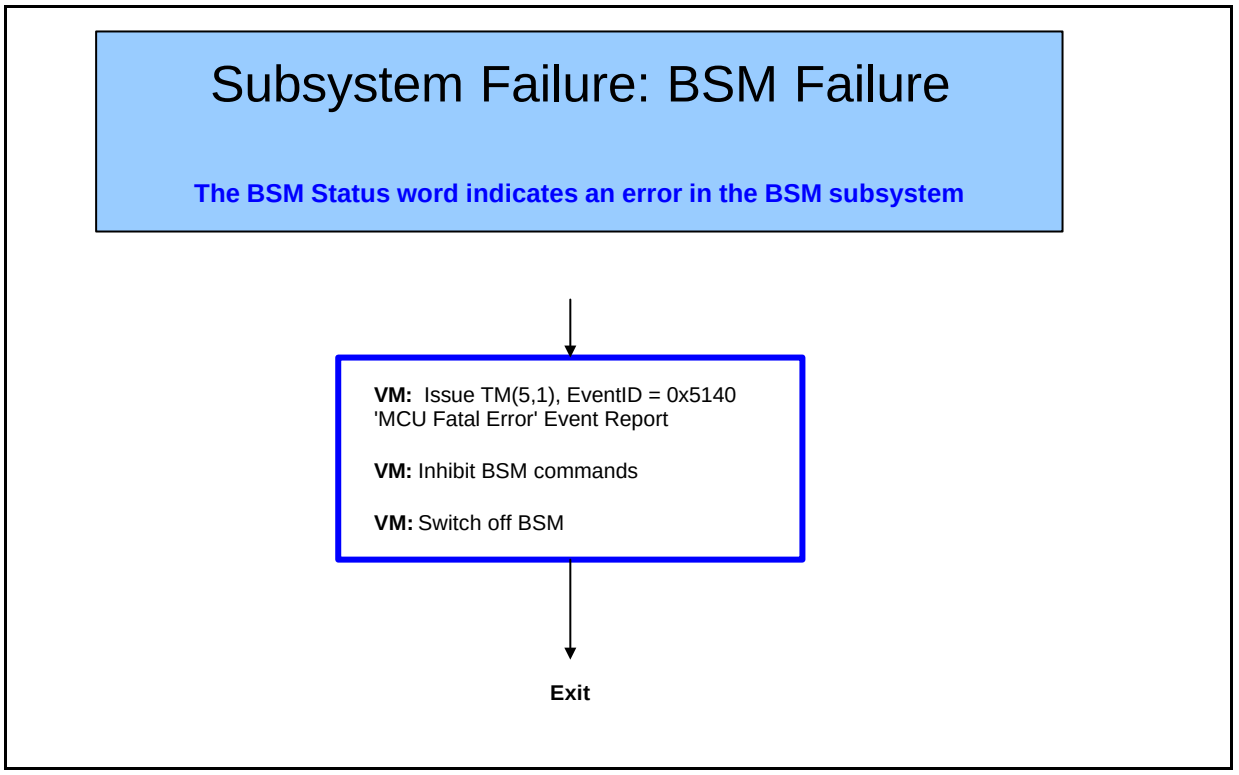
2.7 Calibrators



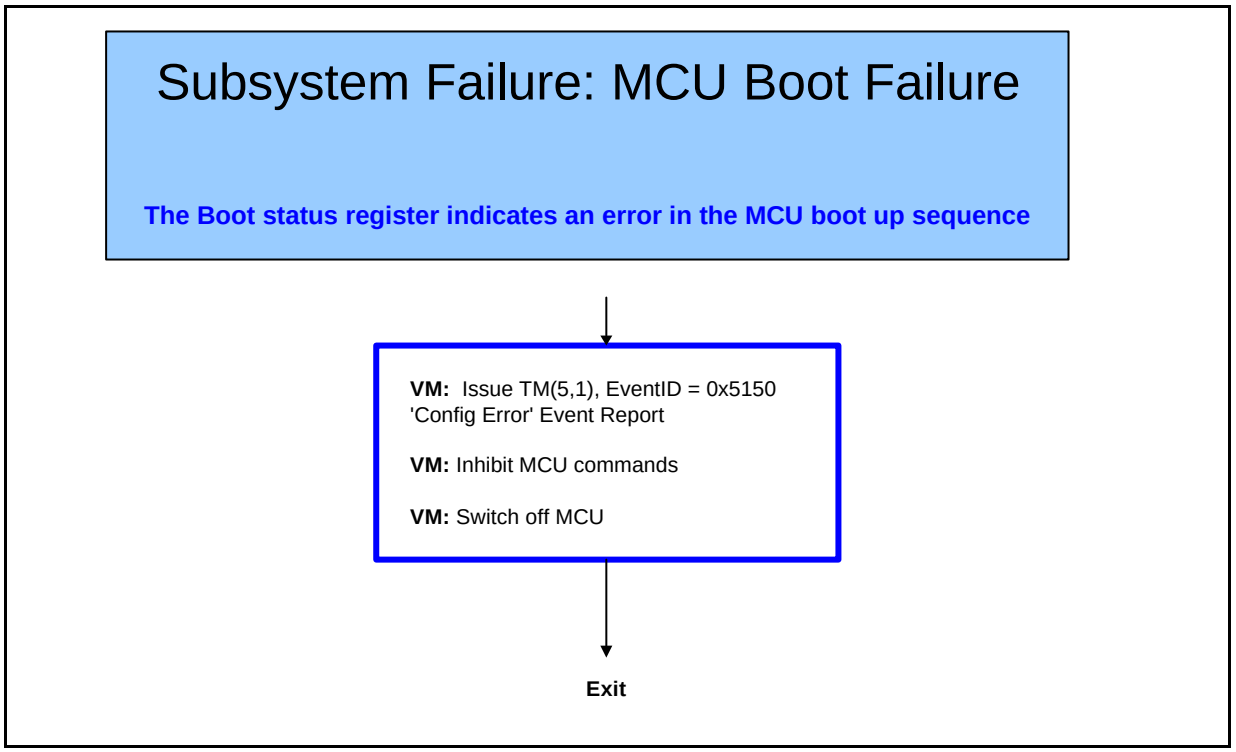
2.8 SMEC


Subsystem Failure: SMEC Failure
The SMEC Status bit 15 indicates an error in the SMEC subsystem
VM: Issue TM(5,1), EventID = 0x5140 'MCU Fatal Error' Event Report
VM: Inhibit SMEC commands
VM: Switch off SMEC
Exit

2.9 BSM


Subsystem Failure: BSM Failure
The BSM Status word indicates an error in the BSM subsystem
VM: Issue TM(5,1), EventID = 0x5140 'MCU Fatal Error' Event Report
VM: Inhibit BSM commands
VM: Switch off BSM
Exit

2.10 MCU DSP


Subsystem Failure: MCU Boot Failure
The Boot status register indicates an error in the MCU boot up sequence
VM: Issue TM(5,1), EventID = 0x5150 'Config Error' Event Report
VM: Inhibit MCU commands
VM: Switch off MCU
Exit

2.11 DCU

No specific DCU monitoring has been identified

3. DRCU INTERFACES

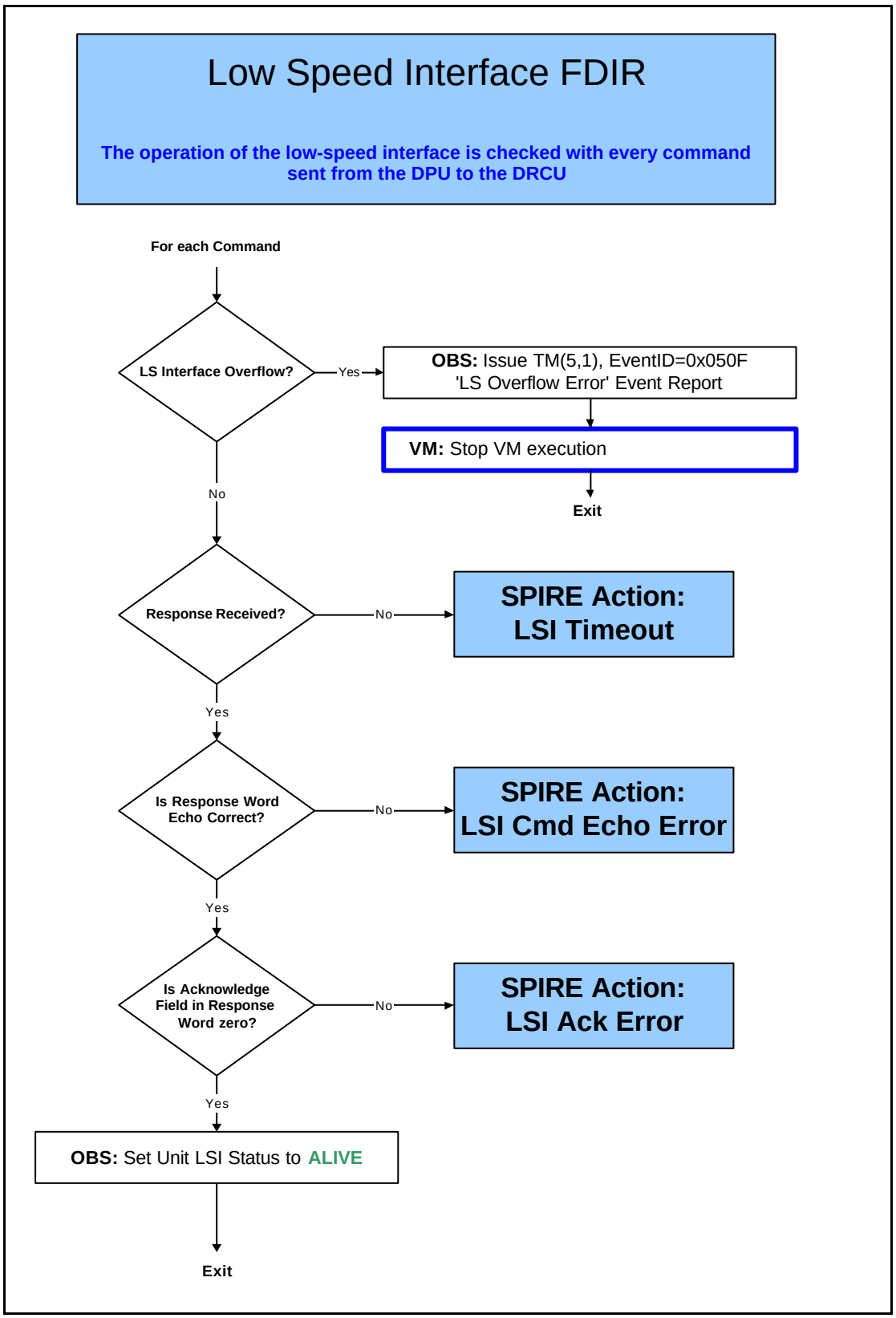
Subsystems are commanded and monitored through data passing through the interfaces with the DRCU. These interfaces have to be checked to be operating correctly before correct operation of the instrument can be expected.

The DRCU contains three units; the DCU, MCU and SCU, and each one has one slow speed interface (used to send commands to the unit and to collect housekeeping parameters) and one high speed interface (used to transfer science data from the unit to the DPU).

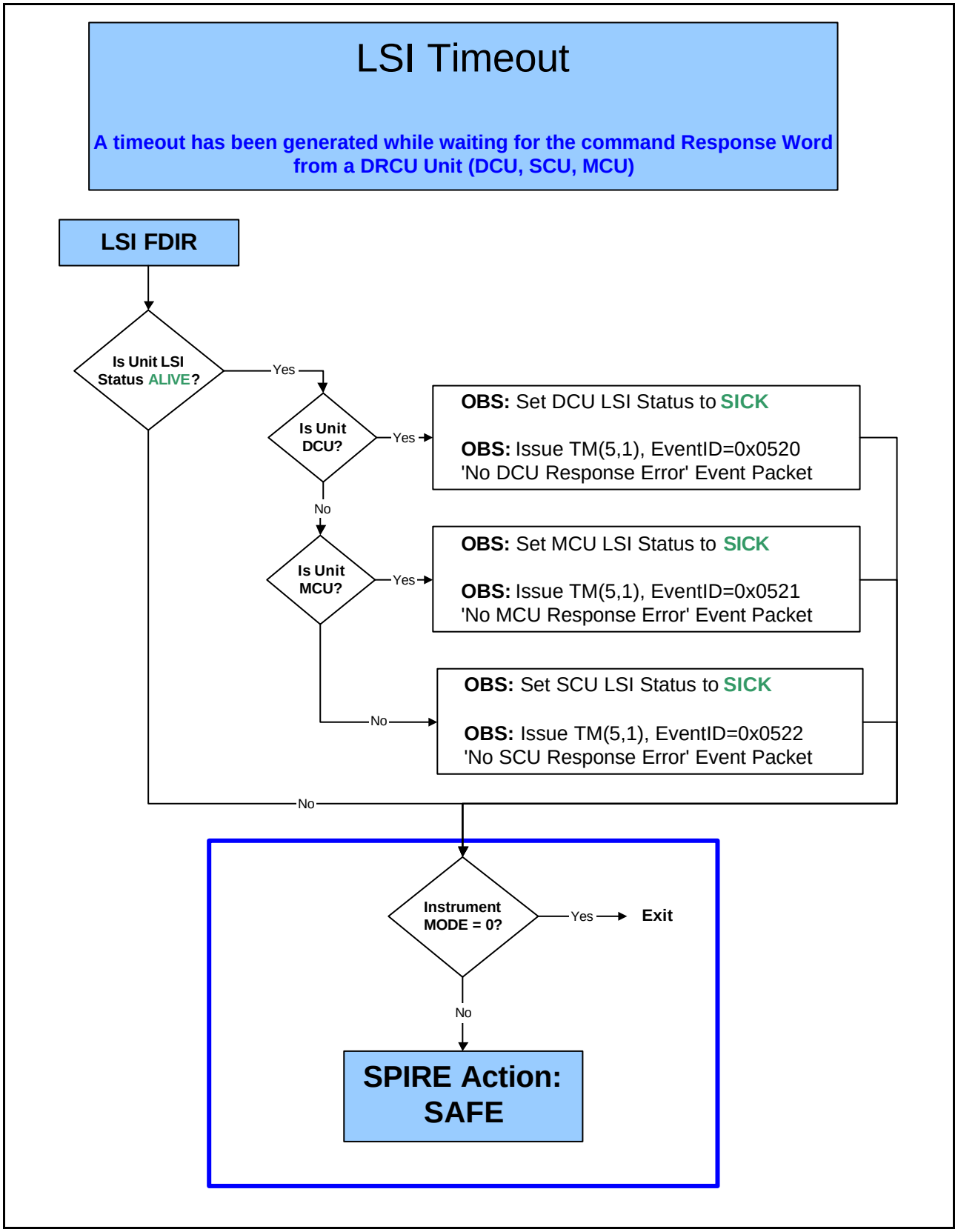
3.1 Low Speed Interface Failures

For each command sent through the LSI a series of checks is made to ensure that the command has been executed correctly. In the event of failure the command is repeated a set number (LSIMax) of times before a failure is declared.

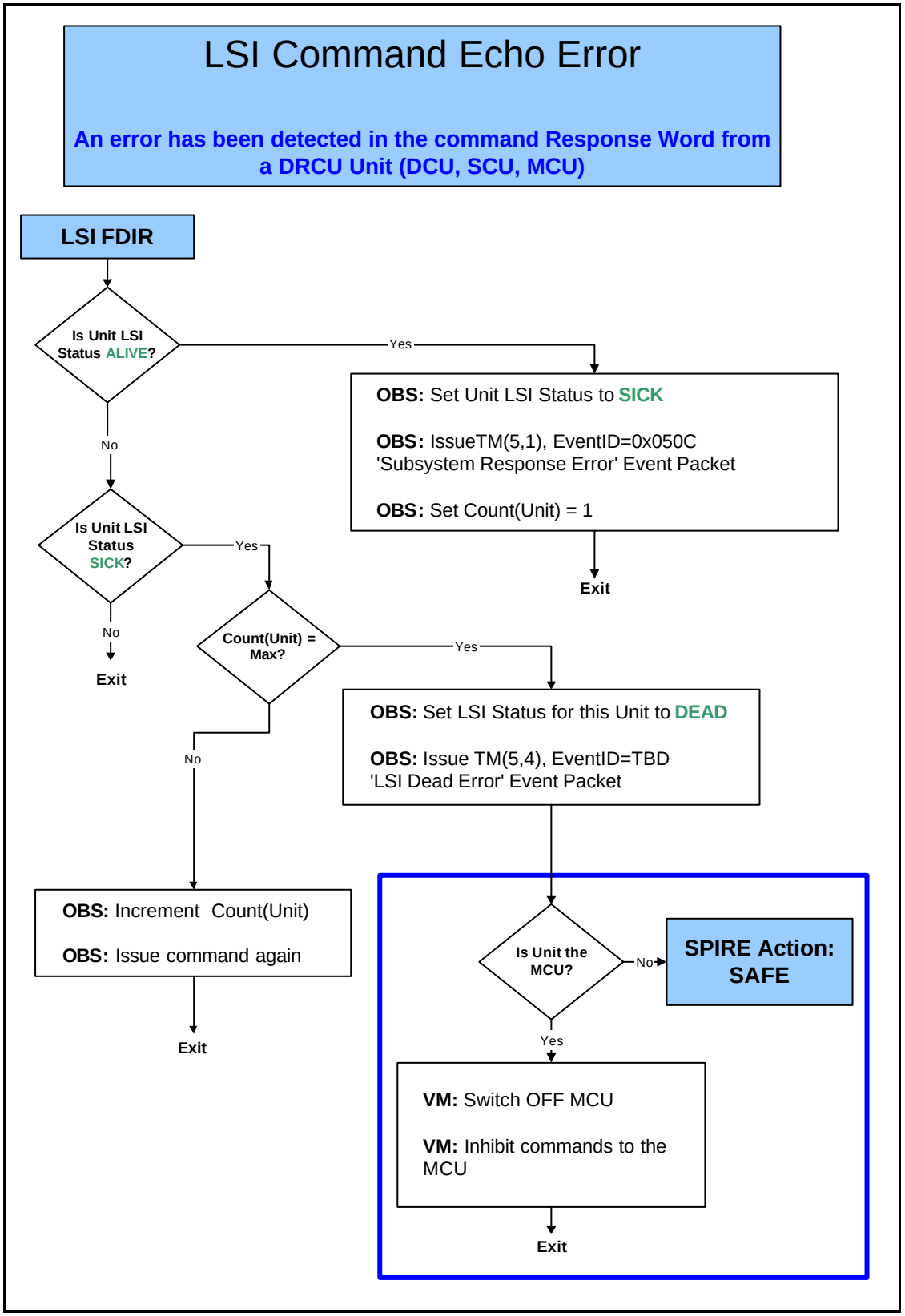
RespMax is set to zero on initialisation of the autonomy system


Low Speed Interface FDIR
The operation of the low-speed interface is checked with every command sent from the DPU to the DRCU
For each Command
LS Interface Overflow?
Yes
OBS: Issue TM(5,1), EventID=0x050F 'LS Overflow Error' Event Report
VM: Stop VM execution
Exit
No
Response Received?
No
SPIRE Action: LSI Timeout
Yes
Is Response Word Echo Correct?
No
SPIRE Action: LSI Cmd Echo Error
Yes
Is Acknowledge Field in Response Word zero?
No
SPIRE Action: LSI Ack Error
Yes
OBS: Set Unit LSI Status to ALIVE
Exit

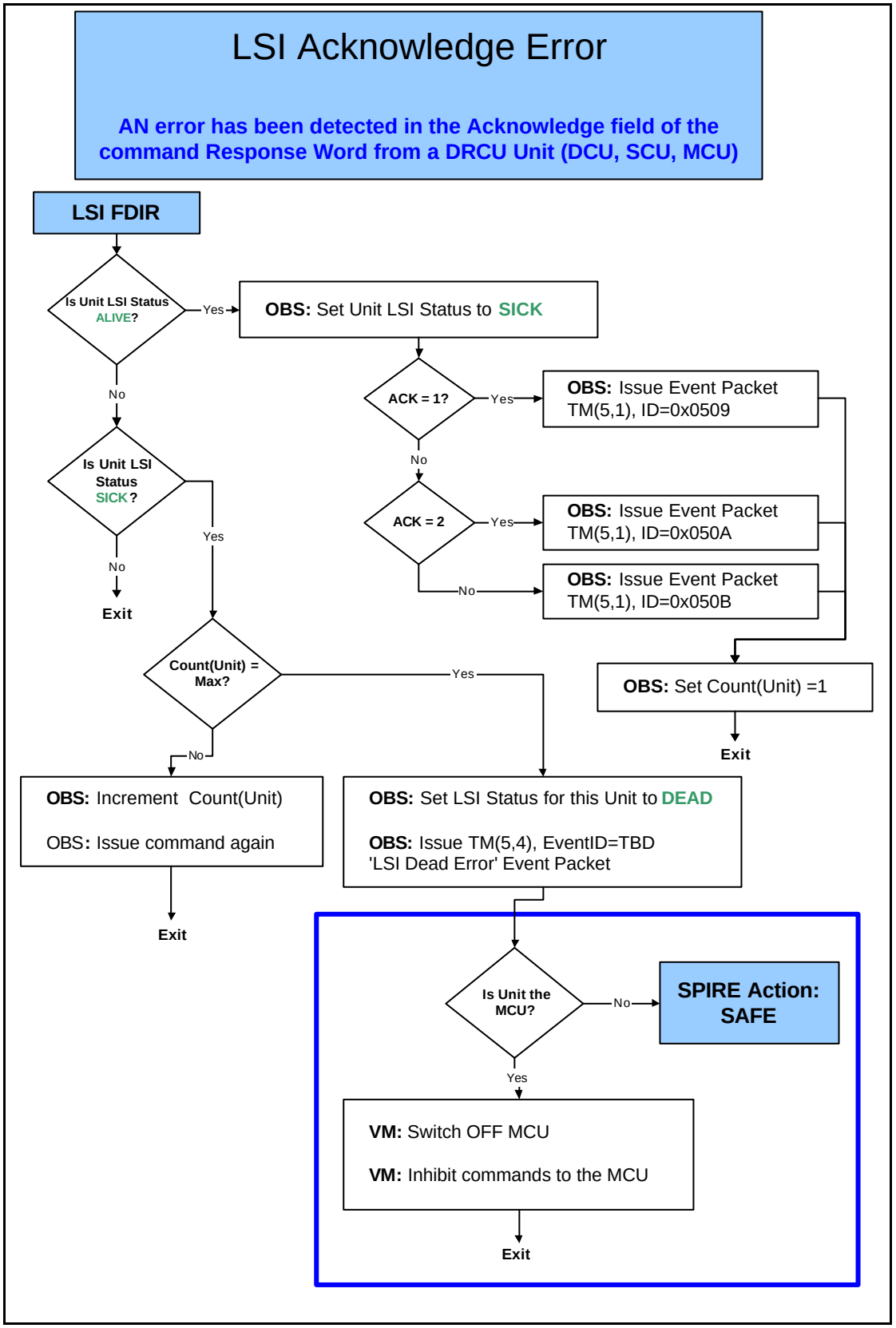
3.1.1 LSI Timeout



3.1.2 LSI Response



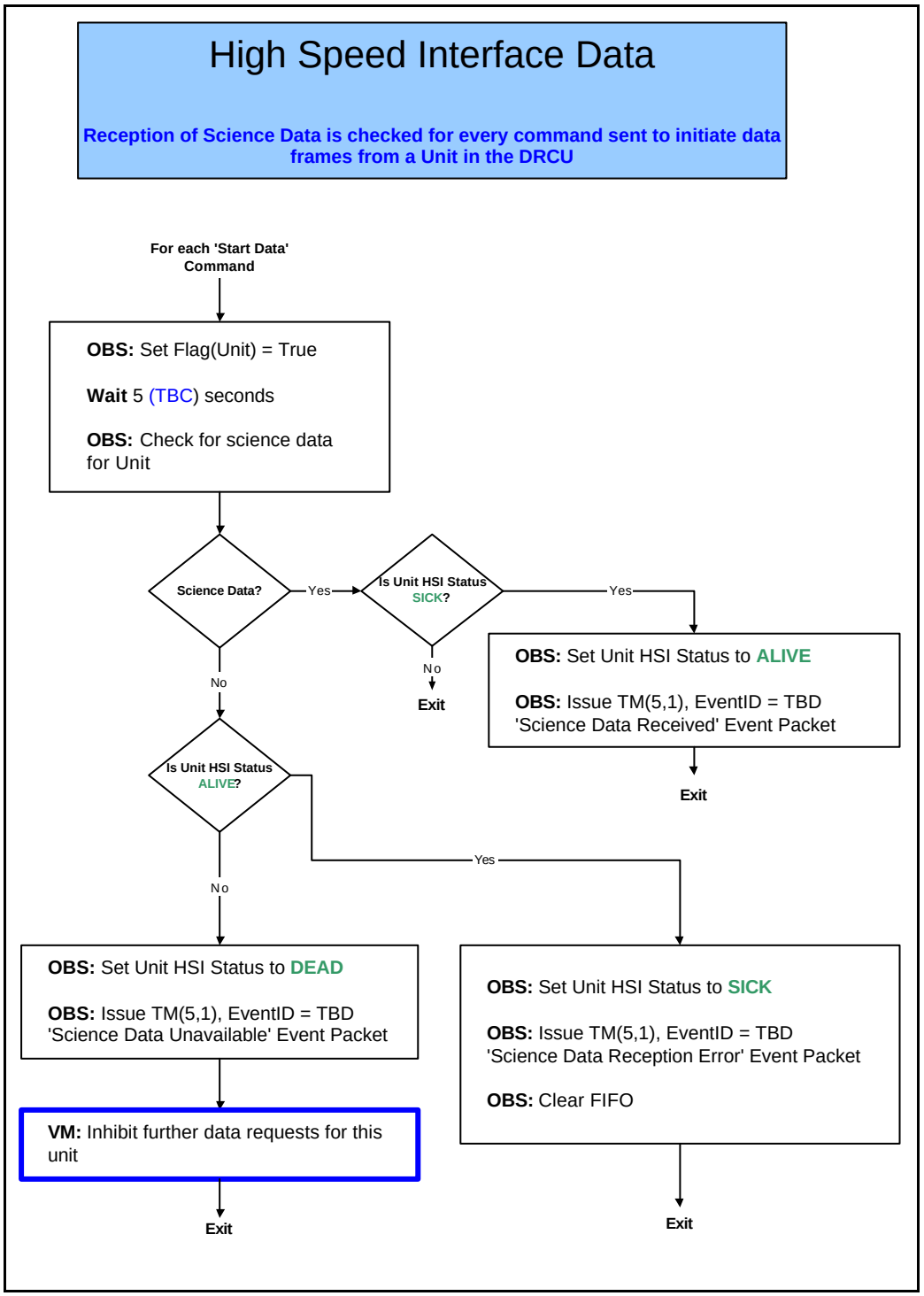
3.1.3 LSI Acknowledge



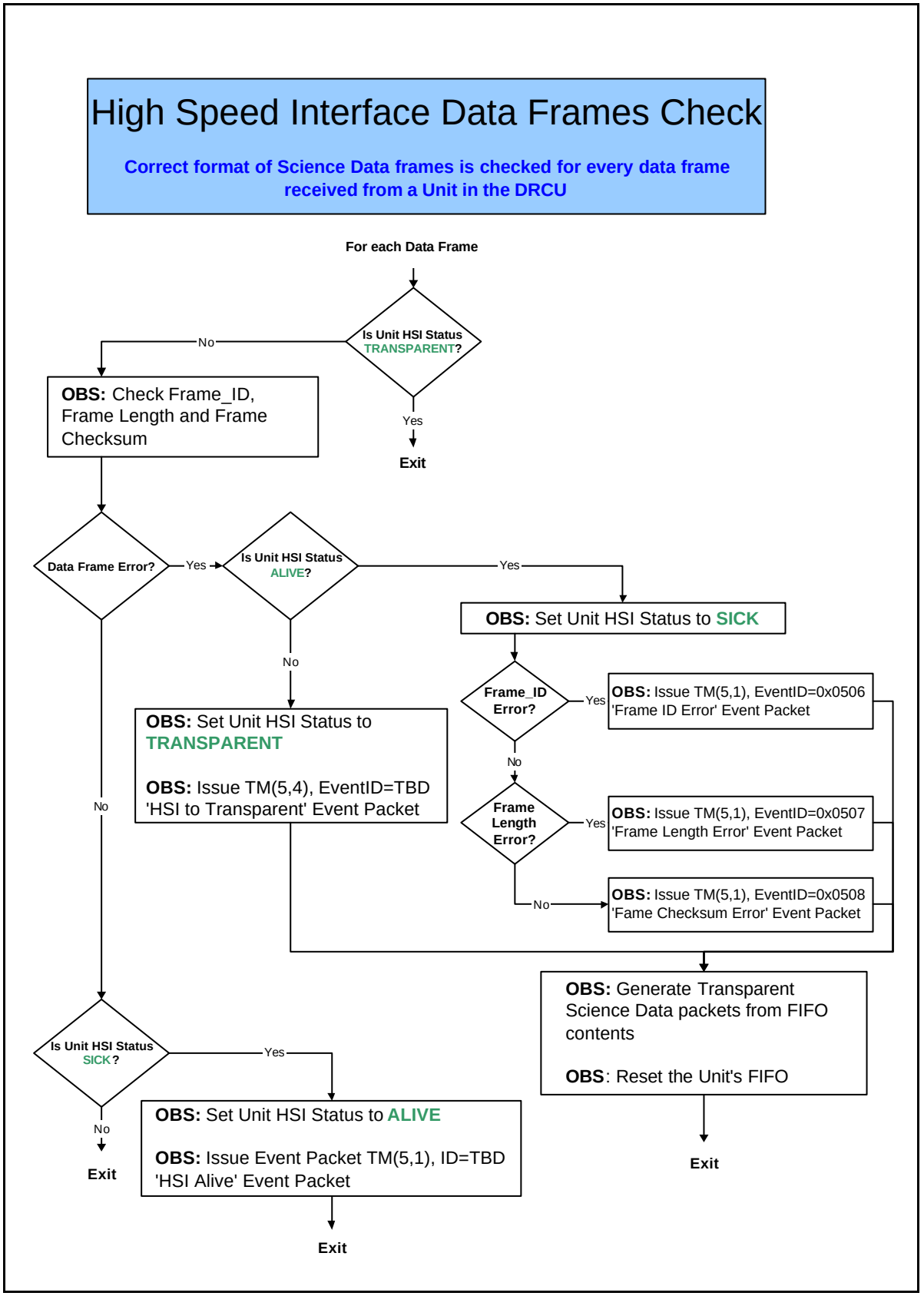
3.2 High Speed Interface Failures

The high speed interfaces transfer science data from the DRCU units to the DPU. Data is collected by the DPU into FIFO buffers which trigger the DPU to empty them when they are half full.

3.2.1 HSI Data

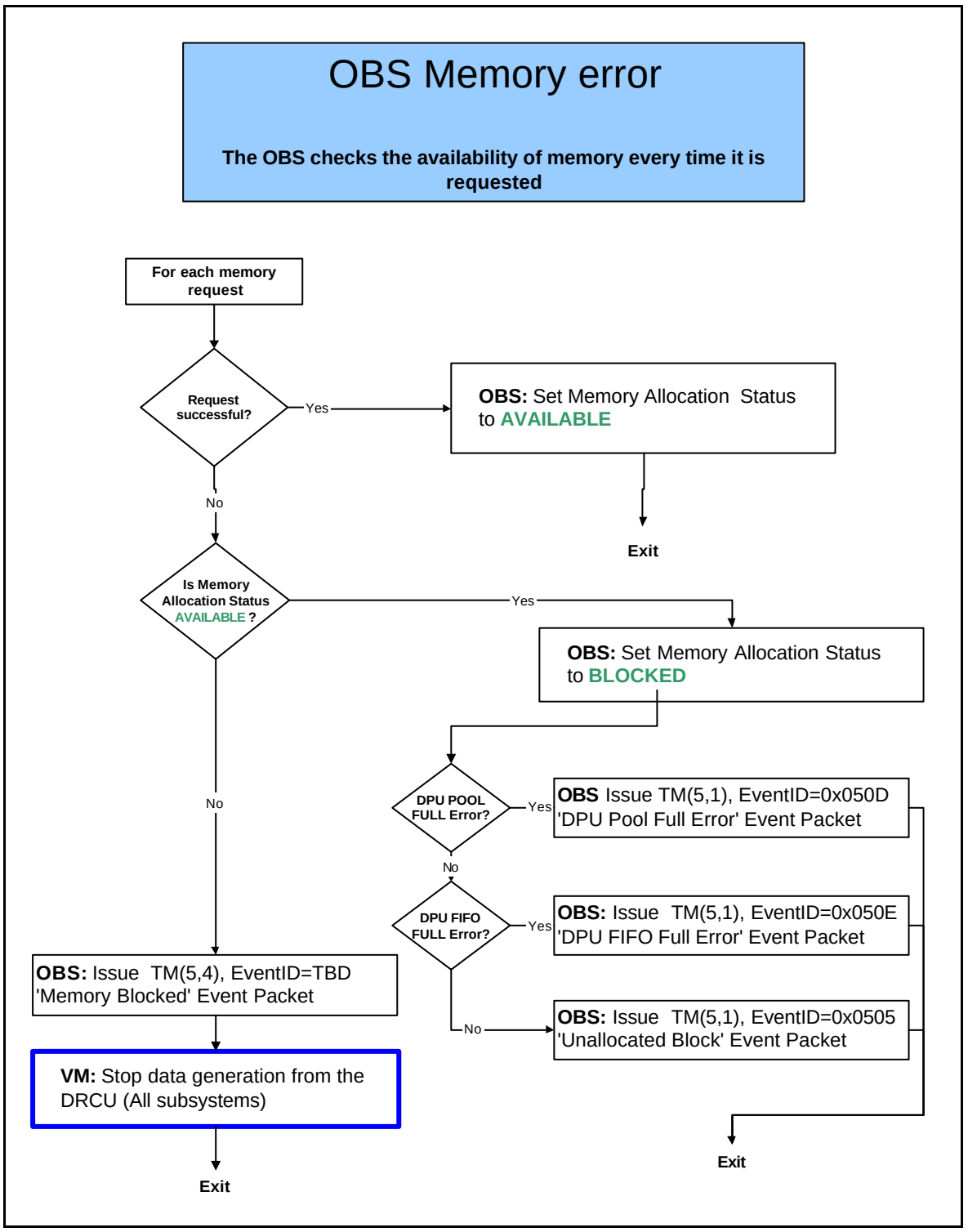


3.2.2 HSI Frames

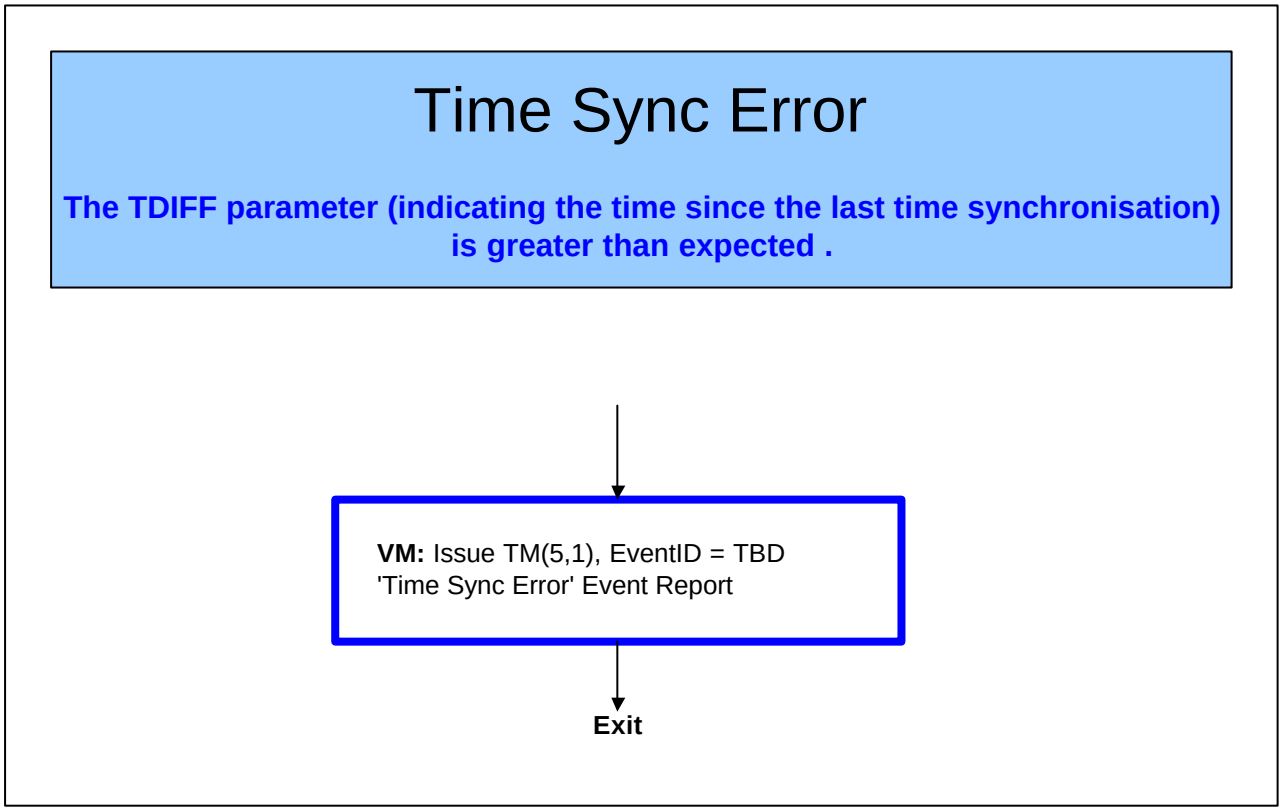


4. OBS RUNTIME ERRORS

4.1 Memory Errors



4.2 Time Sync Error

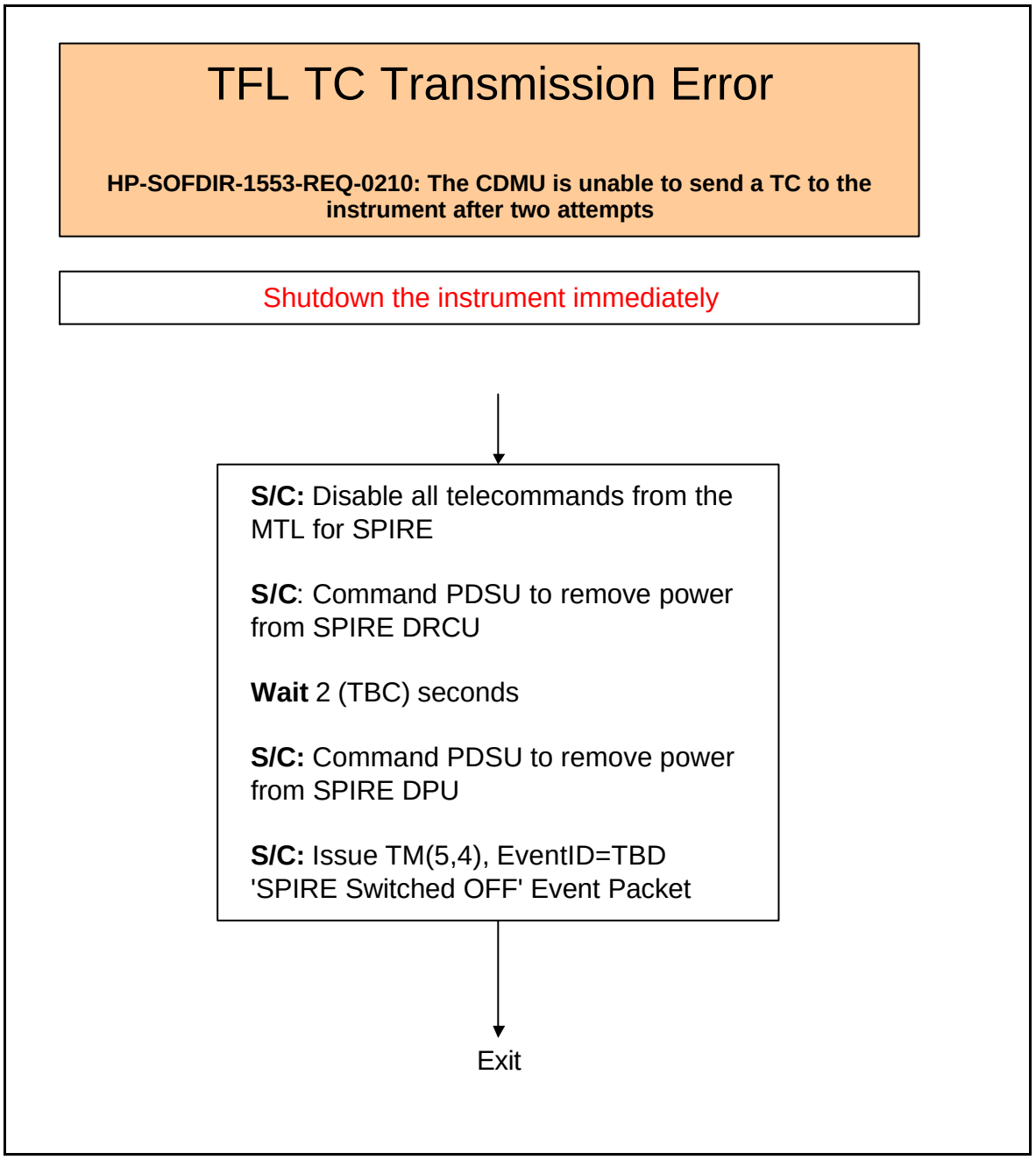


5. S/C INTERFACE

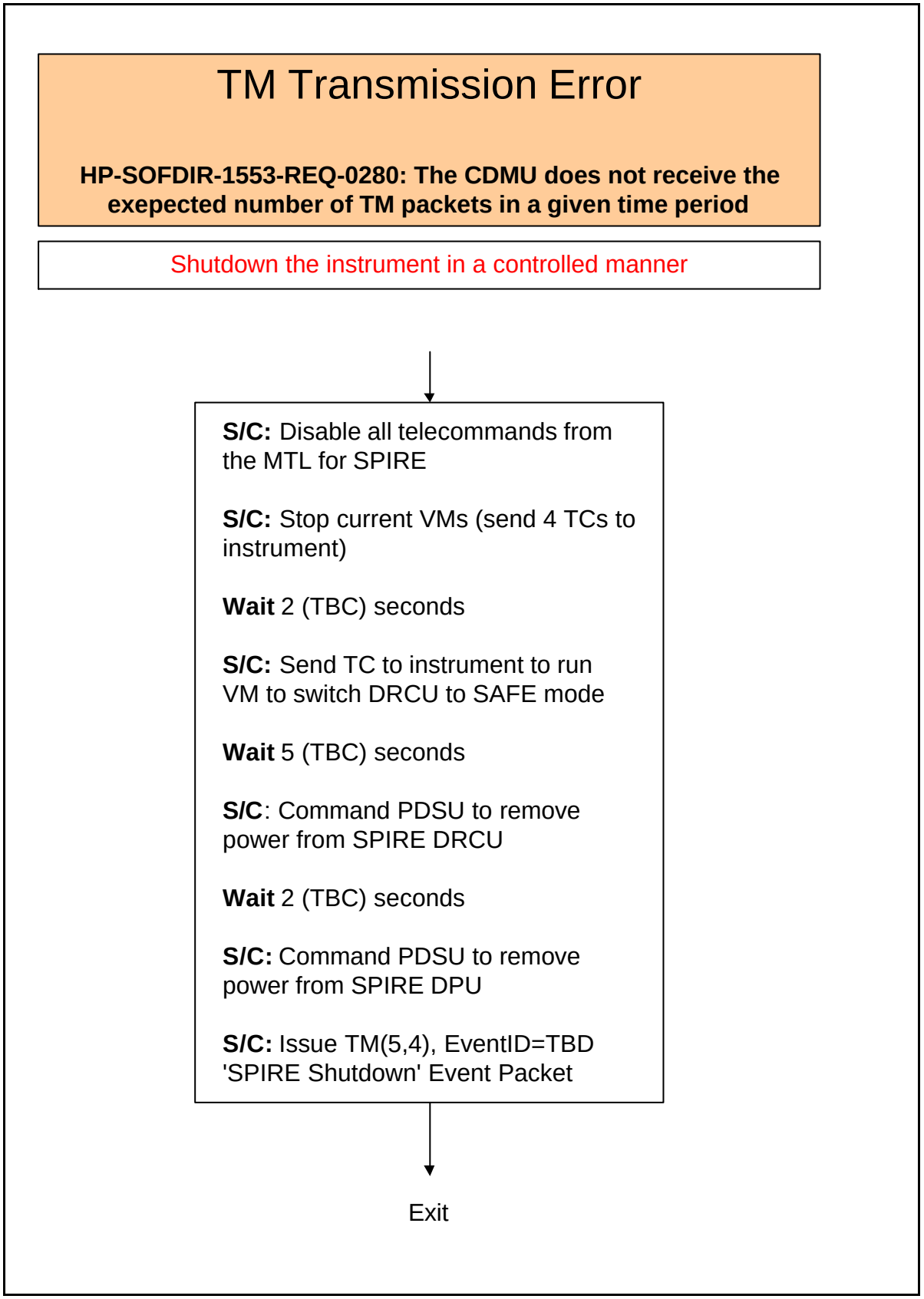
5.1 Bus Failures

Detected by the S/C SOFDIR

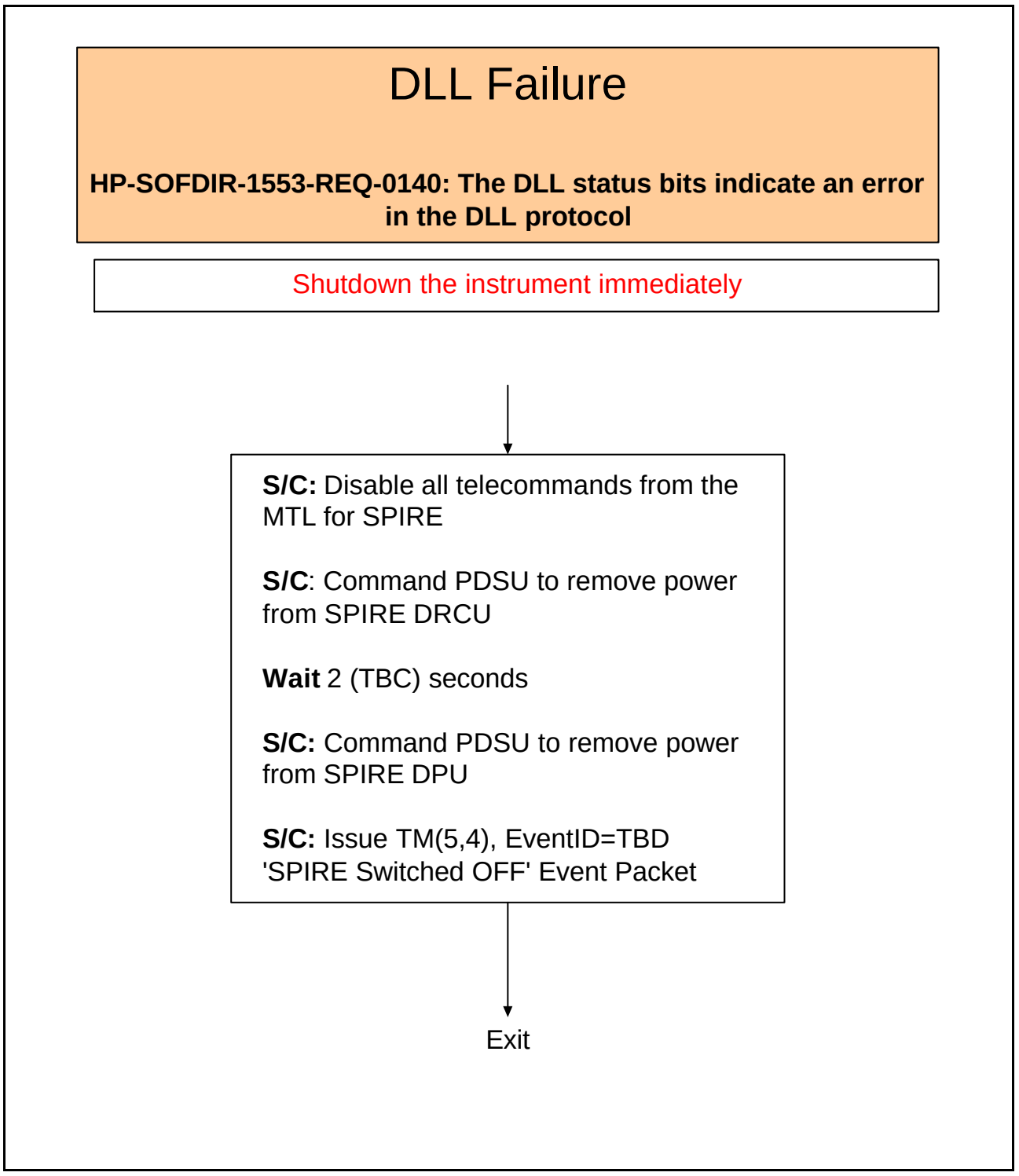
5.1.1 TC Transmission



5.1.2 TM Transmission

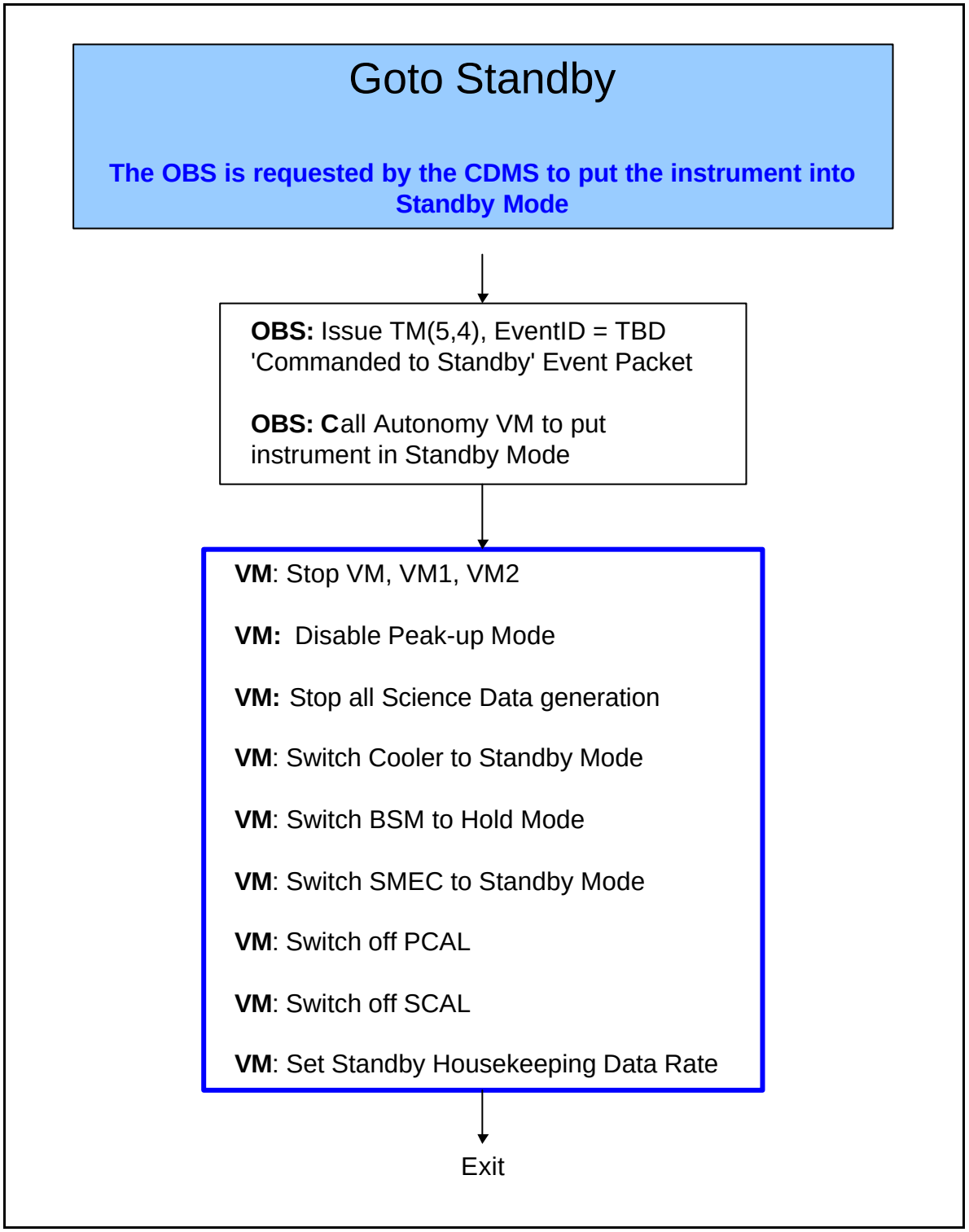


5.1.3 DLL


DLL Failure
HP-SOFDIR-1553-REQ-0140: The DLL status bits indicate an error in the DLL protocol
Shutdown the instrument immediately
S/C: Disable all telecommands from the MTL for SPIRE
S/C: Command PDSU to remove power from SPIRE DRCU
Wait 2 (TBC) seconds
S/C: Command PDSU to remove power from SPIRE DPU
S/C: Issue TM(5,4), EventID=TBD 'SPIRE Switched OFF' Event Packet
Exit

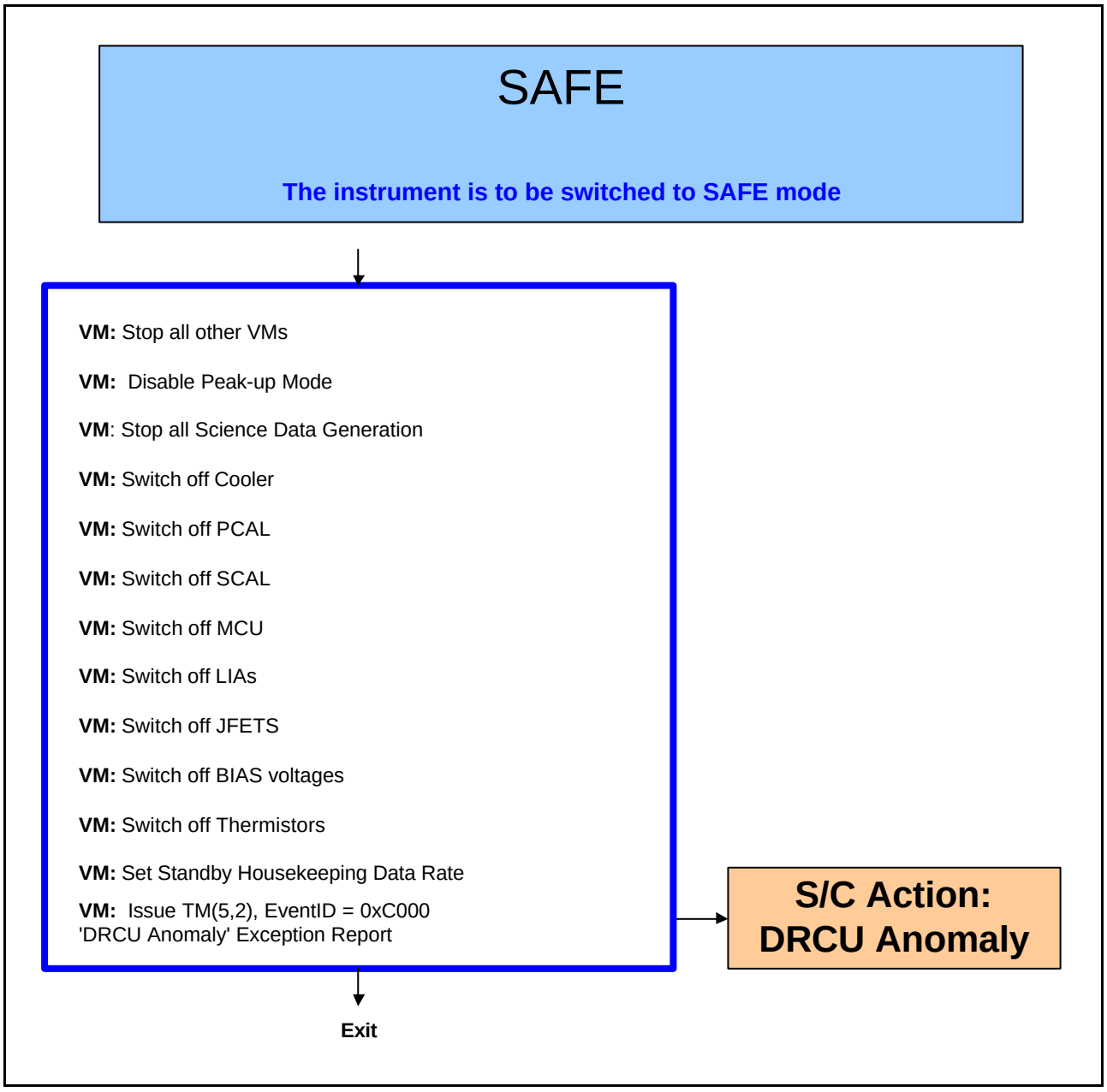
5.2 Spacecraft Commands

5.2.1 Go to Standby

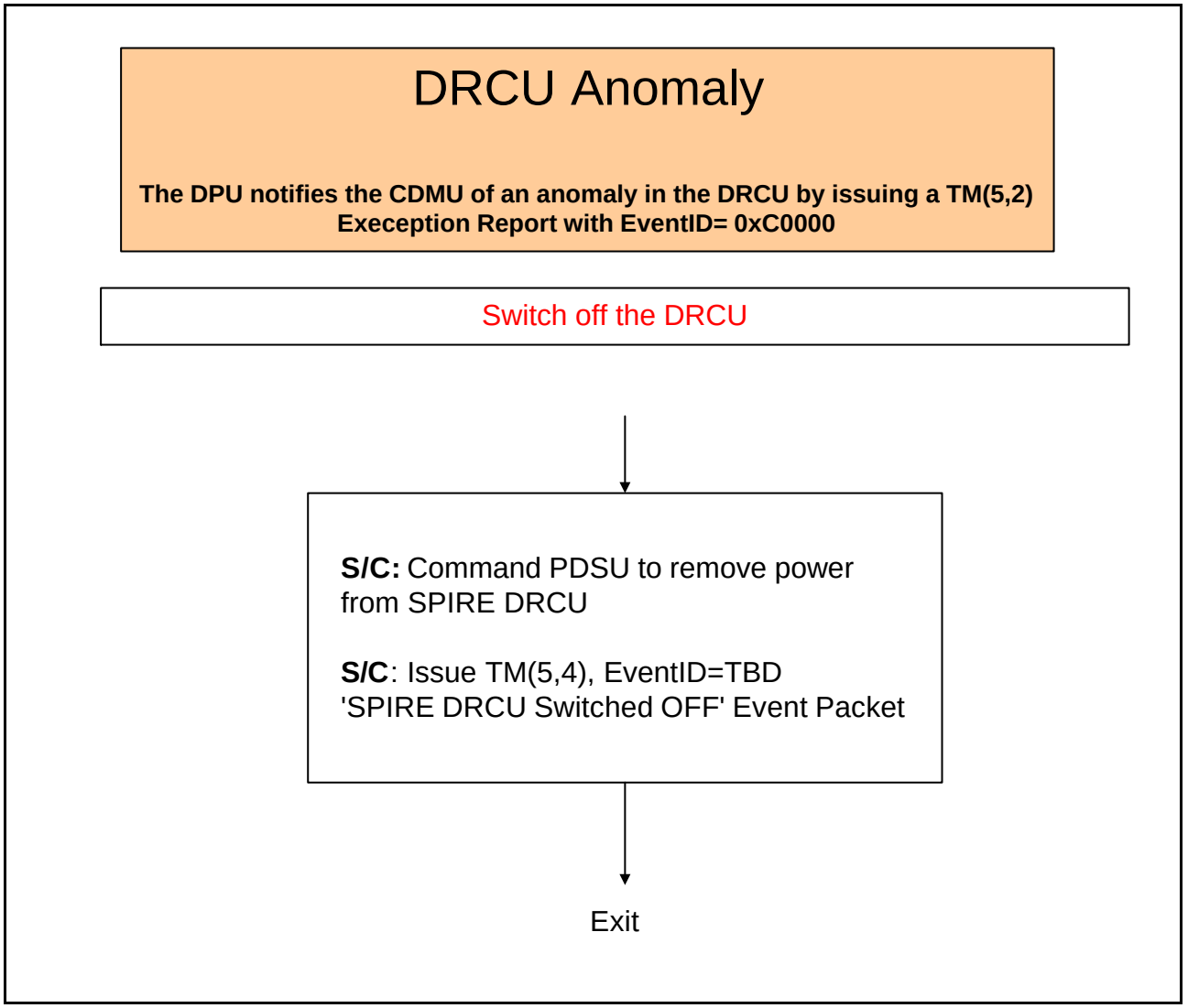


6. GENERAL PURPOSE PROCEDURES

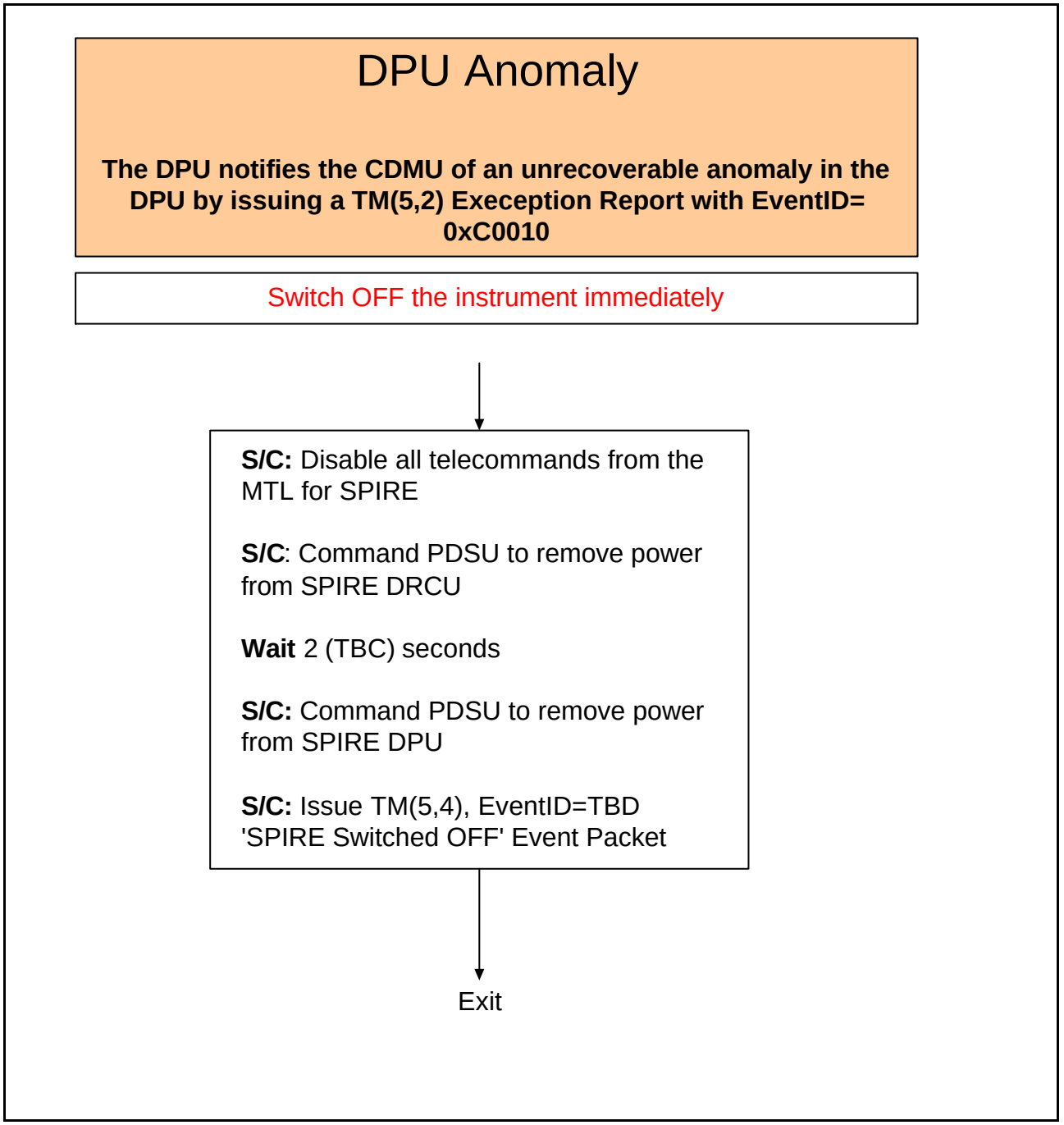
6.1 SAFE



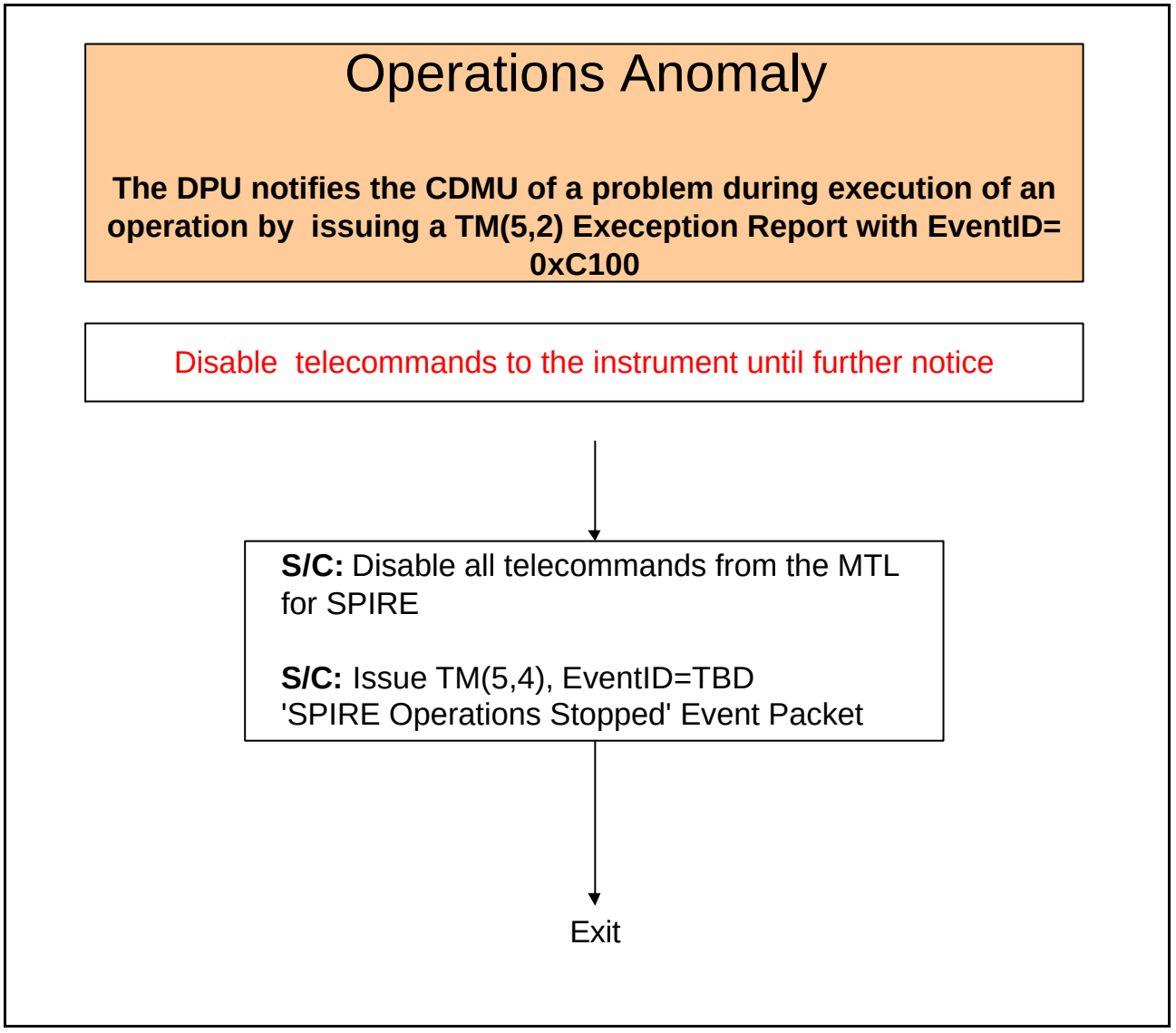
6.2 DRCU Anomaly



6.3 DPU Anomaly



6.4 Operations Anomaly



6.5 Operations Resume