HERSCHEL

DPU/ICU Switch-ON Procedure

Document Ref.: CNR.IFSI.2001TR01

Issue: 1

Prepared by: R.Orfei Date: 12/10/2001
Riccardo Cerulli-Irelli
Anna Maria Di Giorgio

Distribution List :

MPE	O.Bauer		N.Gradmann	
	PACS-PPO			
CSL	E.Renotte		J.M.Gillis	
IAC	J.Herreros			
RAL	K.King			
SRON	K.Wafelbakker		L.Dubbeldam	
	D.Beintema		P.Roelfsema	
CGS	A. Longoni			
IFSI	R. Cerulli Irelli		S. Molinari	
	C.Codella			
	A. Di Giorgio			
	S. Pezzuto			

Document Status Sheet:

Document Title: Herschel DPU/ICU Switch-ON Procedure

Issue	Revision	Date	Reason for Change
Draft 1		23 January 2001	First Draft
Draft2		30 January 2001	2nd draft, containing comments from SPIRE
Draft 3		16/03/2001	3rd Draft, with comments from CDMS WG and CGS
Issue1		12/10/2001	Updating after PS-ICD updating

Document Change Record :

Document Title: Herschel DPU/ICU Switch-ON Procedure	
Document Reference Number: CNR.IFSI.2001TR01	
Document Issue/Revision Number: Issue 1	
Section	**Reason For Change**
All	Draft 1
Sect. 2.1.1, 2.1.2	SPIRE Comments taken into account
Sect. 2.1.1, 2.1.2	CDMS WG and CGS comments taken into account
	Issue 1
Sect. 1.1	Updated
Sect. 1.2.1	Added acronym for ASW, CDMU, CGS, HIFI, PACS, TBD, TBW, TC, TM; corrected CDMS, removed HSO
Sect. 2	Fig. 2.1 updated
Sect. 2	Last part of the section updated
Sect. 2.1.2:	Changes due to new PS-ICD Issue
PROM-ON04.3	updated
PROM-ON04.5	updated
PROM-ON04.6	updated
PROM-ON05	updated
PROM-ON06.5	updated

PROM-ON07	updated
PROM-ON08	updated
PROM-ON09	updated
PROM-ON09.4	updated
PROM-ON09.5	updated
PROM-ON010	updated
PROM-ON013.1	updated
PROM-ON014	updated

1 INTRODUCTION

1.1 Purpose of the document

The Istituto di Fisica per lo Spazio Interplanetario (IFSI) of the Italian Consiglio Nazionale delle Ricerche (CNR) is responsible for the design and manufacturing of the three Digital Processing/Instrument Control Unit for the three instruments to be flown on board of the ESA satellite Herschel: PACS, HIFI and SPIRE.

This specification defines the requirements for the performances, the design and the qualification of the PROM software, which is a CGS deliverable to IFSI.

1.2 Acronyms and Abbreviations

1.2.1 Acronyms

AD	Architectural Design
ASW	Application SW
ATP	Acceptance Test Plan
AVM	Avionic Model
CNR	Consiglio Nazionale delle Ricerche
CPP	Common Parts Procurement
CPU	Control Processing Unit
CDMS	Central Data Management System
CDMU	Central Data Management Unit
CGS	Carlo Gavazzi Space SpA
CQM	Cryogenic Qualification Model
DDD	Detailed Design Document
DM	Data Memory
DPU	Digital Processing Unit
EEPROM	Electrically Erasable Programmable Read Only Memory

ESA	European Space Agency
HIFI	Heterodyne Instrument for FIRST
HK	HouseKeeping
HW	HardWare
IBDR	Instrument Baseline Design Review
ICD	Interface Control Document
ICDR	Instrument Critical Design Review
ICU	Instrument Control Unit
DPU	Digital Control Unit
IHDR	Instrument Hardware Design Review
IFSI	Istituto di Fisica dello Spazio Interplanetario
ISVR	Instrument Science Verification Review
NA	Not Applicable
OBS	On-Board Software
PA	Product Assurance
PACS	Photoconductor Array Camera and Spectrometer
PROM	Programmable Read Only Memory
RAM	Random Access Memory
SCC	SpaceCraft Components
SEU	Single Event Upset
SPIRE	Spectral and Photometric Imaging Receiver
S/S	SubSystem
SVM	Service Module
SW	SoftWare
TBC	To Be Confirmed
TBD	To Be Defined
TBW	To Be Written
TC	TeleCommand
TM	TeleMetry
TV	Thermal Vacuum

1.3 REFERENCES

1.3.1 Applicable Documents

Document Reference	Name
AD1	FIRST/Planck Instrument Interface Document Part A
AD2	FIRST/Planck Instrument Interface Document Part B Instrument “PACS”
AD3	FIRST/Planck Instrument Interface Document Part B Instrument “HIFI”
AD4	FIRST/Planck Instrument Interface Document Part B Instrument “SPIRE”
AD5	PS-ICD
AD6	DPU/ICU OBS PA Plan
AD6	HIFI DPU/ICU OBS URD
AD6	SPIRE DPU/ICU OBS URD
AD6	PACS DPU/ICU OBS URD

1.3.2 Reference Documents

Document Reference	Name

1.4 Introduction

The present document is intended to provide the requirements for the functions/routines to be implemented by the PROM, that is the part of the OBS that is executed at the DPU/ICU switch on and that could allow a recovery of the situation, should a permanent corruption of some RAM memory locations occur.

2 General DPU/ICU description

In the following figure 2-1 the general block diagram of the DPU/ICU is shown together with the dimensions of the different memories, namely:

- PROM 32 Kbyte
- EEPROM 1 Mbyte
- Program Memory 3 Mbyte
- Data Memory 2 Mbyte.

The DSP 21020 has a "Harvard Architecture" so that Data Memory Bus and Program Memory Bus are completely separated, so allowing an increased instruction cycle speed.

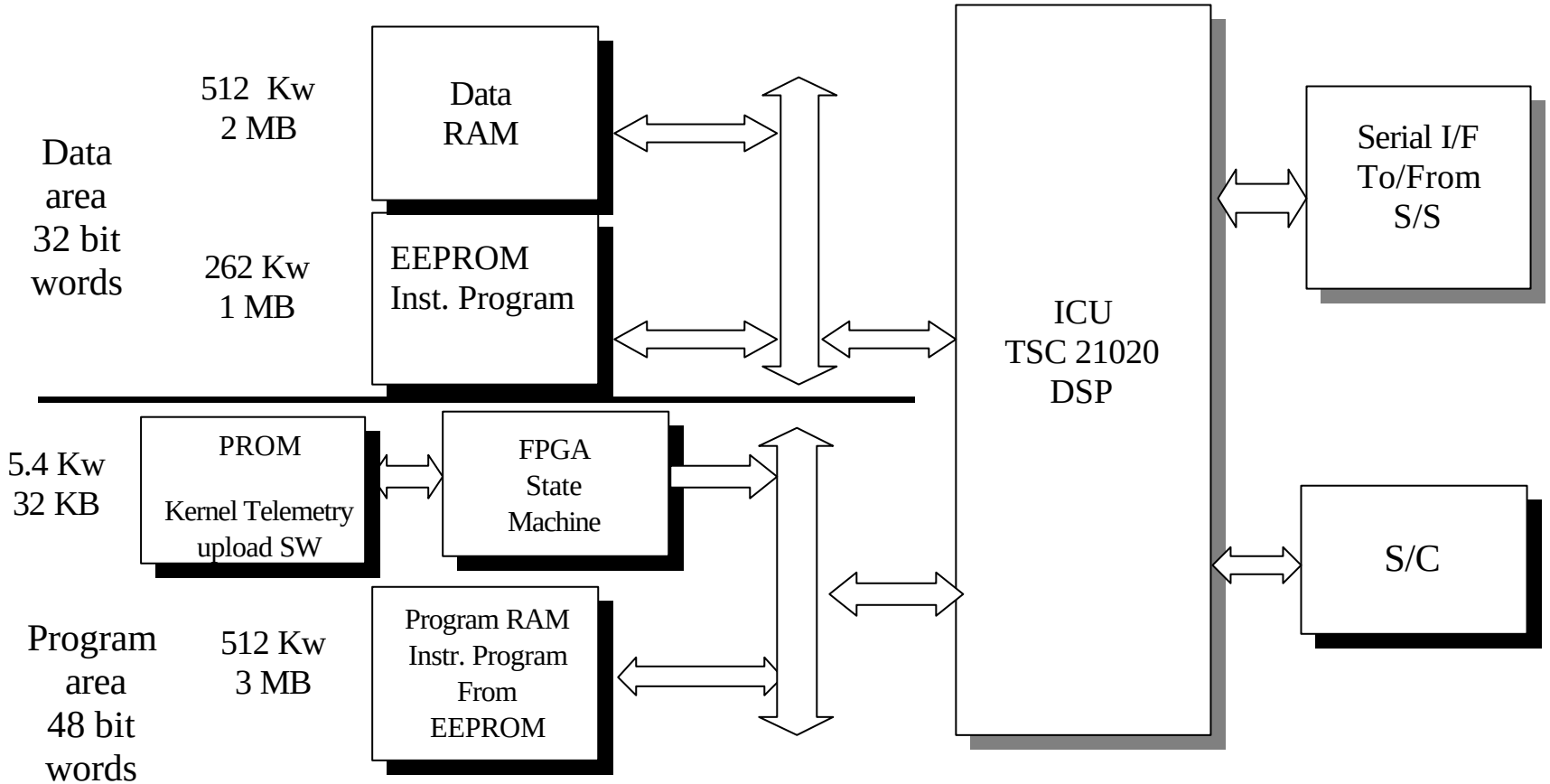
It is also to be noted that:

- after the switch-ON the PROM is loaded via a state machine into the Program Memory;
- the EEPROM is mapped in Data Memory;
- the Data Memory word is 32 Bit wide while the Program Memory word is 48 Bit wide.

2.1 Switch-ON Procedure

In Figure 2-2 the flow diagram of the DPU/ICU Switch-ON procedure is shown.

Figure 2-1 DPU/ICU General Block Diagram



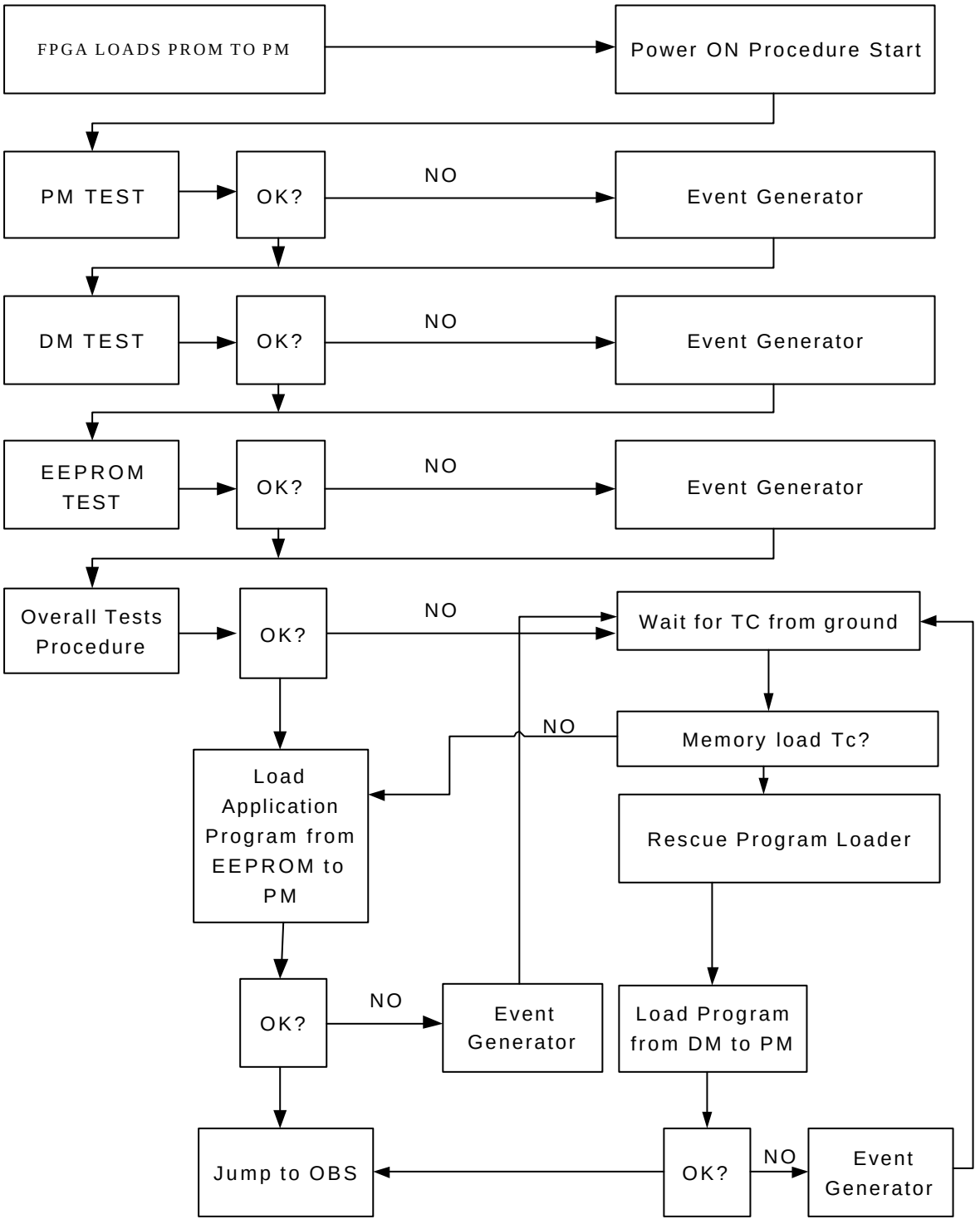


Figure 2-2 Power-ON procedure flow chart diagram

2.1.1 Overall functional description

It is to be noted that the switch-ON procedure of an Herschel instrument can only take place when there is direct link between ground and satellite. If there is one of the failures described in the following, the DPU/ICU is unable to go in the instrument INIT mode, that is, the DPU/ICU is in Rescue Program Loader mode. The S/C CDMU is then expected only to upload a new program image; under these conditions no HK, but only Events can get out of the DPU/ICU.

When the DPU/ICU model is switched ON, that is the relevant 28 V lines dedicated to DPU/ICU are powered, the FPGA device loads the PROM content in the Program Memory while the DSP is kept in a RESET state and thus inactive (Reset is Asserted). At the end of the operation the DSP reset is released (Reset De-asserted) and the DSP starts program execution from the address 0x08: the Power-ON Procedure starts. The first following operation is the test of the Program Memory (of course not the part where the PROM program is located).

An example of the memory cells test sequence can be the following:

- WRITE in location N 0xA5A5A5A5A5A5
- READ and check the content of location N
- WRITE in location N 0x5A5A5A5A5A5A
- READ and check the content of location N
- N=N+1
- Repeat the above sequence.

If the test fails, then the procedure generates a Telemetry Event Packet (Error/Alarm report, see requirement list below) containing mainly the indication of the type of the on-board memory where the check failed, the total number of failures and the ID of the damaged segments. The Program Memory, and this applies also for the Data Memory, can be divided in segments (pages), as an indication 256 segments/pages, in order to avoid a large generation of events if the memory damage is serious.

This damage information could allow the on ground generation of a new software image to be loaded only on valid memory segments.

After the PM test, even if the test failed, the Data Memory test is started: for example the sequence can be the following:

- WRITE in location N 0xA5A5A5A5
- READ and check the content of location N
- WRITE in location N 0x5A5A5A5A
- READ and check the content of location N

- N=N+1
- Repeat the above sequence.

If the test of the DM fails, then the procedure generates a Telemetry Event Packet (Error/Alarm report, see requirement list below) with the same type of information indicated before.

After the DM test , the EEPROM content is checked, but in this case only the check sum(s) will be checked as the EEPROM can only be read (and written again, but this is not taken into account in this procedure). This test can be made by comparing the checksum of the EEPROM pages with the corresponding values reported in the header of each page (TBC).
If the test of the EEPROM fails, then the procedure generates a Telemetry Event Packet (Error/Alarm report, see requirement list below) with the same type of information indicated before.

At the end of the three tests, if just one of them failed, then the procedure starts waiting for a telecommand from ground. The TC can either force the power ON procedure to continue with the next step (load the application program from EEPROM to PM) or start a "Rescue Program Loader" procedure, capable to load the new code image from ground by using the Memory Management service (memory up-load TC). In this case the new executable is first loaded in DATA RAM and then copied from DM to PM in not corrupted/defective memory segments. This will be possible because the new executable will have the same structure as an EEPROM software image, which shall be organised in segments, each of which with its own header containing an indication of the PM address where the segment shall be mapped.
If the procedure of copying the new image from DM to PM fails, as well as in case of error in the reception of the memory load telecommand, the procedure generates an event and starts waiting for a new telecommand from ground.

The new loaded executable shall not be copied in EEPROM at this stage.

If all tests were OK, the next step in the procedure is to copy the OBS (application software) from EEPROM to PM. A new and final check is performed on the program copied in PM, again check sum(s). In case of successful check the program jumps directly to the OBS first location. If this final checksum test fails a new TM Event packet is generated and the procedure waits for a new telecommand from ground.

At the end of the procedure, the program jumps to the OBS first location.

2.1.2 PROM Software High Level Requirements

In this section the list of high level requirements for the implementation of the PROM software is provided. This list is intended to be used as input for the definition of Software requirements and for the definition of the overall (functional and operational) design of the Software.

Req. ID	Description	Reference
PROM-ON01	The PROM S/W shall be started at power-on of the DPU/ICU	IFSI
PROM-ON02	The PROM S/W shall perform the initialisation and checking of the health of the unit, including the following functions: - Program Memory checking (test of all the memory area not occupied by the PROM software) - Data Memory Checking (test of all the memory area not occupied by the PROM software) - EEPROM checking - Configuration and Initialisation of the MIL-STD-1553B link to communicate with the CDMU	
PROM-ON03	For each one of the checks performed, in case of failure an Event Report shall be generated reporting the values specified as per req. PROM-ON04.6.	IFSI
PROM-ON04	The Event Report TM packet shall have a structure compatible with the description in AD5. In particular:	IFSI
PROM-ON04.1	In the Packet Header the following values shall be set for the Packet ID fields (structured according to AD5 section 4.1.1.1): Version Number: '000' (bin) Type: 0 Data Field Header Flag: 1	IFSI
PROM-ON04.2	In the Packet Header - Packet ID the following instrument APIDs shall be inserted: HIFI: APID= 1024 (400h) TBC PACS: APID=1152 (480h) TBC SPIRE: APID=1280 (500h)TBC	IFSI
PROM-ON04.3	In the Packet Header - Packet Sequence Control fields (structured according to AD5 section 4.1.1.2) the following values shall be inserted: Segmentation Flags: '11'(bin) Source Sequence Count (start=1): it is a counter of all the event packets released with the same APID. The value of the counter shall be available	IFSI

	in a dedicated memory location in RAM, in order to be used by the ASW.	
PROM-ON04.4	In the Packet Header - Packet Length field (structured according to AD5 section 4.1.1.3) the number N of bytes contained in the Packet Data Field shall be written as an unsigned integer. N = (number of bytes in packet data field) – 1.	IFSI
PROM-ON04.5	In the Packet Data Field – Data Field header (structured according to AD5 section 4.1.2.1) all the fields shall be filled in with the following values: Spare: 0 TM PUS version number: 0 Spare: 0 Packet Type: 5 Packet Subtype: 4 Spare: 0 Time: MSB=1 meaning not yet synchronised	IFSI
PROM-ON04.6	In the Packet Data Field – Source Data (structured according to AD5 section 5.5.2) the following values shall be reported: *EVENT ID:* (TBD) *SID*: (TBD) Parameters: 1st *Memory checked* (2 MS bits): 01 (PM) 02 (DM) 03 (EEPROM) *Number of failures* (8 LS bits): number of memory pages with failure detected. *2nd and up to 21 parameters* *Pages Ids:* identifier of the corrupted memory page (8 bits per identifier). Up to a maximum of 40 Ids can be sent within one Event report. In case of a number of failures greater than 40, more than one reports shall be issued, containing all the same info apart from the packet length and the Segment Ids.	IFSI
PROM-ON04.7	In the Packet Data Field – Packet Error Control Field (structured according to AD5 section 4.1.2.3) the checksum value of the packet shall be included. The value shall be provided in accordance to a standard error detection encoding/decoding procedure described in AD5, Appendix 4)	IFSI

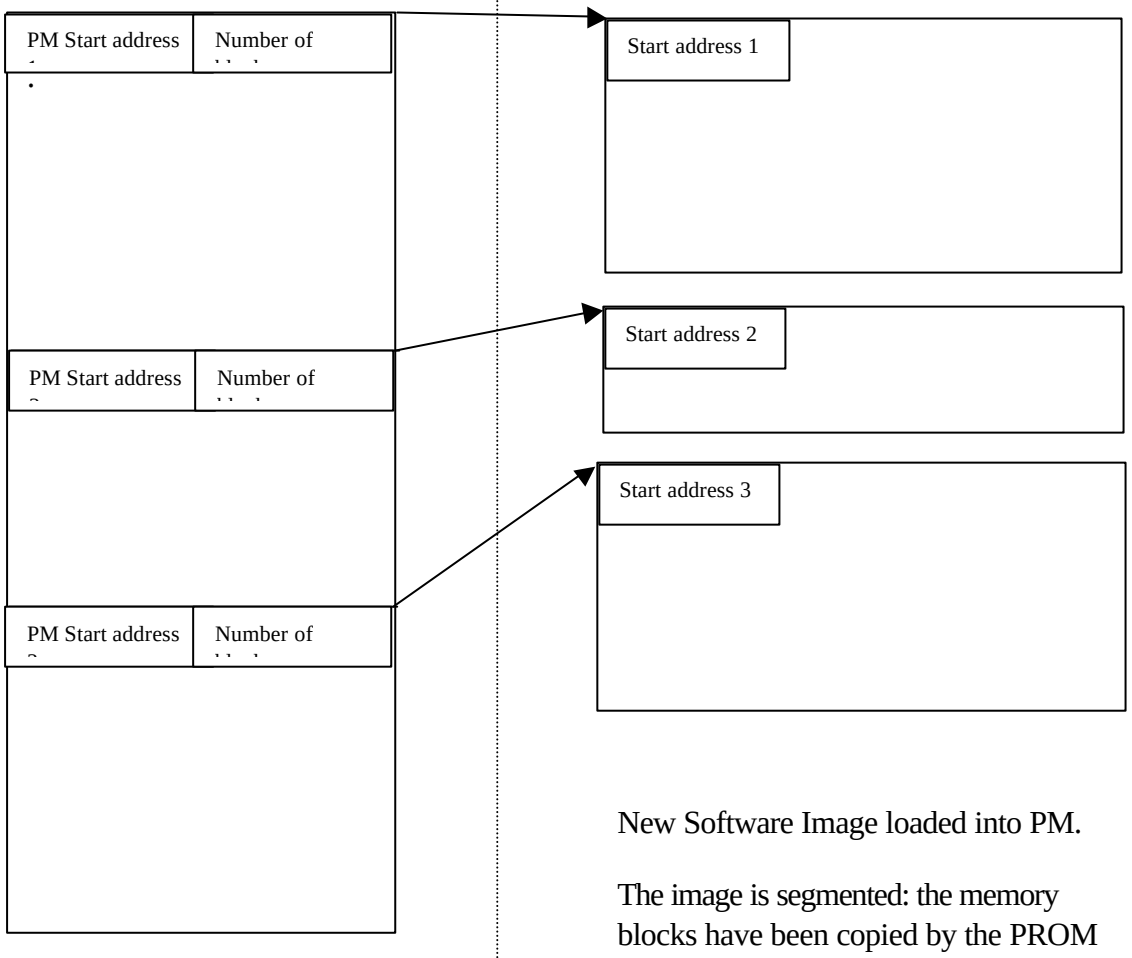
PROM-ON05	In case of one or more failure detection, the Power On procedure shall be able to load via TC a new software image from ground. The TC service to be used for these purposes is the Service Type 6 (Memory Management), subtype 2 (load memory using absolute addresses).	IFSI
PROM-ON06	The Power on procedure shall be able to acquire and execute the Memory Load telecommands structured according to the specifications in AD5 sections 3.1 and 5.6.1. In particular:	IFSI
PROM-ON06.1	The TC Packet Header-Packet ID fields shall contain the following values (AD5 section 3.1.1): Version Number: '000' (bin) Type: 1 Data Field Header Flag: 1 APID : - HIFI: 1024 (400h) TBC - PACS: 1152 (480h) TBC - SPIRE: 1280 (500h)TBC	IFSI
PROM-ON06.2	The TC Packet Header - Packet Sequence Control fields (structured according to AD5 section 3.1.1.2) shall contain the following values: Sequence Flags (2bits): '11'(bin) Sequence Count (14 bits) divided in : - source part (3 most significant bits) = 000 - sequence part (remaining 11bits) = it is a counter of all the TC packets released with the same APID. (no check on the counter consistency shall be performed for the acceptance of the TC)	IFSI
PROM-ON06.3	The TC Packet Header - Packet Length field (structured according to AD5 section 3.1.1.3) shall contain the number N of bytes contained in the Packet Data Field. N = (number of bytes in packet data field) – 1.	IFSI
PROM-ON06.4	In the TC Packet Data Field – Data Field header (structured according to AD5 section 3.1.2.1) all the fields shall contain the following values: CCSDS Secondary header Flag (1bit): 0 TM PUS version number: 0 Ack: 0 (TBC – see requirement PROM-ON08 Packet Type: 6 Packet Subtype: 2 Spare: 0	IFSI
PROM-ON06.5	The TC Packet Data Field – Application Data field (structured	IFSI

	according to AD5 section 5.6.1.2) will contain the following values: *Memory ID* (16 bits), destination memory block (DM). Memory ID = 255 indicates that the memory loading is concluded. No data field is foreseen in this case (TBC). *Start Address* (16 bits): relative start address in the destination memory block (DM). The actual start address is made up of 24 bits, where the MS 8 bits are sent as the LS 8 bits of the Memory ID. The address is in SAU (4 bytes for DRAM, 6 bytes for PRAM). *Length* (16 bits): number of SAU to be loaded, MS 8 bits spare. *Data:* memory image to be loaded (one word after the other, where the word length in bytes depends on the destination memory block) *Checksum*: CRC checksum generated over the data block. The Power ON procedure will analyse the checksum according to a standard error detection encoding/decoding procedure described in AD5, Appendix 4. In case of wrong checksum, the Power On procedure shall generate an Error/Alarm event Report and stop running the Emergency Program loader routine.	
PROM-ON06.6	The Packet Data Field – Packet Error Control Field (structured according to AD5 section 4.1.2.3) shall contain the checksum value of the whole TC packet. The Power ON procedure will analyse the checksum according to a standard error detection encoding/decoding procedure described in AD5, Appendix 4. In case of wrong checksum, the Power On procedure shall generate an Error/Alarm event Report, shall stop running the Emergency Program loader routine and start waiting for a new telecommand.	IFSI
PROM-ON07	The Error/Alarm report shall be structured according to the requirement PROM-ON04 and all its sub-requirements. The only difference is in the Packet Data Field – Source Data in which the following values shall be reported: *Event ID: 16 bits TBD* *SID (16 bits)*: TBD *Memory ID* (16bits): the same as the one of the Memory load TC where the error was detected. See PROM-ON06.5 *Start address* (16bits): the same as the one of the Memory load TC where the error was detected. See PROM-ON06.5 *Checksum ID (2 bits):* type of checksum field where the error was detected (1 = data block checksum; 2 = packet checksum) *Checksum value read* (16 bits): value of the checksum read in the TC	IFSI

	Checksum value calculated (16 bits): value of the checksum calculated on board (TBC).	
PROM-ON08	The Power ON procedure will accept and execute the TC without any TC acceptance protocol. This "emergency" procedure is the only case in which the TC acknowledge acceptance of the packet shall not be generated. (TBC).	IFSI
PROM-ON09	The Power on procedure shall be able to acquire and execute TC messages of the type "Function Management – perform an activity of a function (8,4)" structured according to the specifications in AD5 sections 5.8.1.4. This is used to command instrument actions. In particular:	IFSI
PROM-ON09.1	The TC Packet Header-Packet ID fields shall contain the following values (AD5 section 3.1.1): Version Number: '000' (bin) Type: 1 Data Field Header Flag: 1 APID : - HIFI: 1024 (400h) TBC - PACS: 1152 (480h) TBC - SPIRE: 1280 (500h)TBC	IFSI
PROM-ON09.2	The TC Packet Header - Packet Sequence Control fields (structured according to AD5 section 3.1.1.2) shall contain the following values: Sequence Flags (2bits): '11'(bin) Sequence Count (14 bits) divided in : - source part (3 most significant bits) = 000 - sequence part (remaining 11bits) = it is a counter of all the TC packets released with the same APID. (no check on the counter consistency shall be performed for the acceptance of the TC)	IFSI
PROM-ON09.3	The TC Packet Header - Packet Length field (structured according to AD5 section 3.1.1.3) shall contain the number N of bytes contained in the Packet Data Field. N = (number of bytes in packet data field) – 1.	IFSI
PROM-ON09.4	In the TC Packet Data Field – Data Field header (structured according to AD5 section 3.1.2.1) all the fields shall contain the following values: CCSDS Secondary header Flag (1bit): 0 TM PUS version number: 0 Ack: 0 (TBC – see requirement PROM-ON08	IFSI

	Packet Type: 8 Packet Subtype: 4 Spare: 0	
PROM-ON09.5	The TC Packet Data Field – Application Data field (structured according to AD5 section 5.8.1.4) will contain the following values: *Function ID* (8 bits) = TBD it identifies the command for the procedure to continue loading the application program from EEPROM to PM. *Activity ID* (8 bits): TBD	IFSI
PROM-ON09.6	The Packet Data Field – Packet Error Control Field (structured according to AD5 section 4.1.2.3) shall contain the checksum value of the whole TC packet. The Power ON procedure will analyse the checksum according to a standard error detection encoding/decoding procedure described in AD5, Appendix 4. In case of wrong checksum, the Power On procedure shall generate an Error/Alarm event Report and start waiting for a new telecommand.	IFSI
PROM-ON10	The PROM Software shall communicate with the CDMS through a MIL_STD-1553B link according to the protocols defined in appendix 9 of the PS_ICD document [AD5]. In particular, the PROM SW shall be able to send TM messages of the type "Event Reporting, Error/Alarm report (5,4)" as specified in Section 5.5.2 of AD5 and to receive TC messages of the type Memory Management – Load Memory using Absolute Address (6,2) as specified in section 5.6.1.2 of AD5. The SW shall also be able to receive TC messages of the type "Function Management – perform an activity of a function (8,4)" as specified in section 5.8.1.4 of AD5.	IFSI
PROM-ON11	The Power ON procedure will perform all the PM and DM memory check procedures in a non destructive way. See section 2.1.1 for an indication of the sequence of operations to be performed for the test of each memory cell.	IFSI
PROM-ON12	The Power On procedure shall manage the EEPROM memory in pages.	IFSI
PROM-ON13	The Power On procedure shall be able to copy the new loaded software image from DM to PM, i.e. it shall be able to deal with a segmented software image, where each segment has its own header containing the PM destination address.	IFSI
PROM-ON13.1	The Power On procedure shall be able to check if the copying procedure (either from RAM to PM or from EEPROM to PM) was	IFSI

	successful, i.e. it shall be able to perform a CRC checksum (according to the algorithm described in AD5, Appendix A.4) on each software image segment and to compare it with the value reported in the header of the segment. Should the copying procedure fail an Event report (5,4) shall be issued. See PROM-ON04 with a different Event ID and SID TBD.	
PROM-ON14	The Power On procedure shall be able to jump to the starting address of the Application SoftWare. This address will be included in one header of the ASW.	IFSI



New Software Image loaded into the DM.

The image is not segmented: the memory blocks have been loaded one after the other in the order they have been received

New Software Image loaded into PM.

The image is segmented: the memory blocks have been copied by the PROM Software at the locations indicated.

Figure 2-3 Loaded Memory mapping on the Program memory.