Title:

SD2 Software

User Requirement Document

Project: SHARK - ROSETTA LANDER

Contract: ASI-TS 67/I.O./97 (WP 4510)

		Function	Name	Signature
Prepared	By :	Engineering	P.Bologna	
	By :			
Checked	By :	Project Leader	P. G. Magnani	
	By :			
Approved	By :	P.A. Manager	M. Colomba	
	By :	Program Manager	E. Re	
Authorised	By :	General Manager	V. Venturini	

Configuration Management : Rev.: E Date:

Accepted by : _____ _____

CHANGE HISTORY RECORD

Rev. - Reviewed by _____ Date _____

O.M. Approved by _____ Date _____

Change description: First emission.

Rev. A Reviewed by _____ Date 17.05.99

O.M. 614 Approved by _____ Date _____

Change description: Completely revised after internal review.

Rev. B Reviewed by C.Fantinati Date 20.06.1999

O.M. 635 Approved by R.Re Date 20.06.1999

Change description: revised after internal review

Rev. C Reviewed by P.Bologna Date

O.M. 683 Approved by R.Re Date

Change description: updated for new telecommand/ telemetry specification. Added also OCPL

Rev. D Reviewed by P.Bologna Date

O.M. 806 Approved by R.Re Date

Change description: Updated for SD2 FM SW development:

- modified the drill position and the carousel position control
- introduced the new specific commands: LANDG (check the landing gear legs position before starting drilling); DRTT (drill translation with timeout); DRTC (check of drill translation main/ redundant)
- introduced the traceability matrices URD vs system specifications

---

Rev. E Reviewed by P.Bologna Date

O.M. 815 Approved by R.Re Date

Change description: Updated Annex B; the matrix now contains only the SD2 parameter names, while the values of them are contained in SW_Media

REVISION INDEX OF SHEETS

Sheet	1	2	3	4	5	6	7	8	9	10	11	12	13
Rev.	-	-	-	-	-	-	-	-	-	-	-	-	-
Rev.	A	A	A	A	A	A	A	A	A	A	A	A	A
Rev.	B	B	B	B	B	B	B	B	B	B	B	B	B
Rev.	C	C	C	C	C	C	C	C	C	C	C	C	C
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D
Rev.	E	E	E	E	D	D	D	D	D	D	D	D	D

Sheet	14	15	16	17	18	19	20	21	22	23	24	25	26
Rev.	-	-	-	-	-	-	-	-	-	-	-	-	-
Rev.	A	A	A	A	A	A	A	A	A	A	A	A	A
Rev.	B	B	B	B	B	B	B	B	B	B	B	B	B
Rev.	C	C	C	C	C	C	C	C	C	C	C	C	C
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D

Sheet	27	28	29	30	31	32	33	34	35	36	37	38	39
Rev.	-	-	-	-	-	-	-	-	-	-	-	-	-
Rev.	A	A	A	A	A	A	A	A	A	A	A	A	A
Rev.	B	B	B	B	B	B	B	B	B	B	B	B	B
Rev.	C	C	C	C	C	C	C	C	C	C	C	C	C
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D

Sheet	40	41	42	43	44	45	46	47	48	49	50	51	52
Rev.	-	-	-	-	-	-	-	-					
Rev.	A	A	A	A	A	A	A	A	A	A	A	A	A
Rev.	B	B	B	B	B	B	B	B	B	B	B	B	B
Rev.	C	C	C	C	C	C	C	C	C	C	C		
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D
Rev.	D	D	D	D	D	D	D	D	D	D	D	D	D

Sheet	53	54	55	56	57	58	59	60	61	62	63	64	65
Rev.													
Rev.	A	A	A	A	A	A	A	A	A	A			
Rev.	B	B	B	B	B	B	B	B	B	B			
Rev.													
Rev.	D	D	D	D									
Rev.	D	E	E	E									

DISTRIBUTION LIST

Internal Distribution

Name	Copies
E. Re	1
P.G. Magnani	1
R. Gallerini	1

External Distribution

Name	Company	Copies
R. Mugnuolo	ASI – Matera	1
A. Olivieri	ASI – Matera	1

LIST OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

The purpose of this document is to specify the user requirements of the SD2 subsystem flight software. The document describes what shall be expected from software functionality for each mission phase and condition. Special attention is devoted to CDMS interfacing, hardware software interaction and respect to failure handling.

Hardware, processor, firmware and coding limitations relevant to SD2 subsystem are reported to address software development.

Requirements are numbered referring to section and sequence numbers (notation is UR-section-sequence).

All requirements in this specification shall be considered essential.

1.2 SCOPE

This document applies to SD2 flight SW development

1.3 ACRONYMS AND ABBREVIATIONS

AMDT	Acquisition Mode Descriptor Table
CCW	Counter Clock Wise
C-DPU	Common Digital Processing Unit
CDMS	Command & Data Management System
CMD	Command
CW	Clock Wise
EEPROM	Electrically Erasable Programmable Read Only Memory
FIFO	First In First Out
HITB	Historical Internal Tracking Buffer
HK	Housekeeping
I/N	Immediate/Normal Command Type
LM	Laboratory Model
PROM	Programmable Read Only Memory
RAM	Random Access Memory
SD2	Sample Drill & Distribution System
SD2_FSW	SD2 Subsystem Flight Software
S/H	Start/Halt Bit
SSCMD	Subsystem Command Signal
T/R	Transmit/Receive Bit
TRQC	Transmit Request Code Word
WRDC	Word Count
HK_Data	housekeeping data
SC_Data	scientific data
RAM_Data	backup RAM data

1.4 REFERENCE

1.4.1 Applicable documents

AD1 SHARK-ICD-TS-043
CDMS - SD2 Data Interface Control Document

AD2 SHARK-SA-TS-044
SD2 Electronic Unit Internal Interface Control Document

AD3 BSSC(95)2 Issue 1 Draft 2
Guide to applying the ESA Software engineering standards to small software projects

AD4 SHARK-AB-TS-003 SD2 Sub-System specification

1.4.2 Reference documents

RD1 CDMS Subsystems & Instruments Electrical Interface Definition and Generic Payload Control, 27.10.1998

RD2 SHARK-DG-TS-006 SD2 Electronic Unit Specification

RD3 Rosetta Lander Common-DPU User's Manual

RD4 ESA PSS-05-0 ESA Software Engineering Standards (Issue 2, Feb. 1991)

RD5 SD2B-AD-TS-005
SD2 Electronics Unit Acceptance Data Package

1.4.3 Overview

A general description of software under definition is reported in chapter 2. Operations, constraints, references, hardware and operating ambience are generally reported.

Chapter 3 lists what the software has to do and which are its limits and constraints.

Chapter 4 reports a reference addressing to requirements provided by applicable documents.

In Appendixes, position control algorithm, reference values and parameters are reported

2. GENERAL DESCRIPTION

2.1 PRODUCT PERSPECTIVE

SD2 (Drill Sample and Distribution) Subsystem is part of the Rosetta Lander, which is devoted to collect and distribute cometary samples to the on board analysis instruments.

According to CDMS system terminology SD2 is an 'intelligent' unit governed by an own micro-controller unit (C-DPU board). The C-DPU is a universal processor board, designed for the Rosetta Lander experiments. It is based on the radiation hardened RTX2010 processor from Harris. (RTX2000 for LM) Refer to RD3 for more details.

The software hereunder defined (SD2_FSW, SD2 Flight Software) is in charge to manage SD2 Subsystem behaviour and to interface it with CDMS.

The main tasks requested to SD2_FSW are:

- To receive commands from CDMS
- To manage SD2 operations
  - To perform drill operation
  - To perform cometary material sampling
  - To distribute cometary samples to scientific instruments
  - To supervise operation correctness and acquire housekeeping data
- To transmit execution and housekeeping data to CDMS.

From a general point of view, the SD2 Subsystem is slave of CDMS. Its operations and states are conducted by the CDMS. Also input power supply lines and SD2 internal power sub-switches are activated by the CDMS.

During the Rosetta mission, different phases are foreseen. Principally they are: cruise (hibernation), comet approach, lander separation and descent, and on-comet operation. During various phases, the different systems are switched on and off for maintenance and test or for full operation.

The SD2 Subsystem is not operative if power is switched OFF.

2.2 USER CHARACTERISTICS

The Rosetta Lander Mission Control Centre is the user of SD2_FSW.

Commands generated by EARTH and transferred to Lander or generated by On-board computers, are received by SD2_FSW, during different mission phases, to perform mission objectives.

2.3 GENERAL CONSTRAINTS

The SD2_FSW shall be written using FORTH language.

The C-DPU processor comes with a built-in FORTH compiler.

(Referring to RD3) The software development system provided together with the Common-DPU Laboratory Model is based on FORTH-83.

FORTH is more than a high-level computer language: It is an operating system, a set of development tool and a software design philosophy[1,2]. For the RTX2000/2010 it is even the assembler language with the ability of executing multiple FORTH instructions within one single machine cycle.

The Common-DPU software is located in the main following FORTH screens:

RTX2000r.SCR	– RTX2000 core
	– Standard FORTH-83 dictionary
BIOS.SCR	– Serial terminal I/O
	– CDMS I/O
	– ADC and MUX routines
APPLICAT.SCR	– user application
	– main interpreter loop

The provided BIOS realises the following functions.

- Full CDMS interface support
- ADC and multiplexer control (to manage analog signal acquisition from C-DPU)
- Serial terminal interface control (to manage serial RS232 interface [provided only for the LM] devoted to software development and test).

The requirements hereunder reported are relevant to the “user application” part.

2.4 ASSUMPTIONS AND DEPENDENCIES

All requirements stated hereunder are derived from AD1, AD2 AD4 and their relative applicable documents.

[1] Leo Brodie: „Starting Forth“, Prentice Hall Inc, 1984, 1987, ISBN 0-13-843087-X

[2] Leo Brodie: „Thinking Forth“, Prentice Hall Inc, 1986, ISBN 0-13-917584-9

2.5 OPERATIONAL ENVIRONMENT

SD2 Subsystem interfaces external systems by means the CDMS connection and it receives power from the Power System. A general connection block diagram is reported in Fig. 2.5-1.

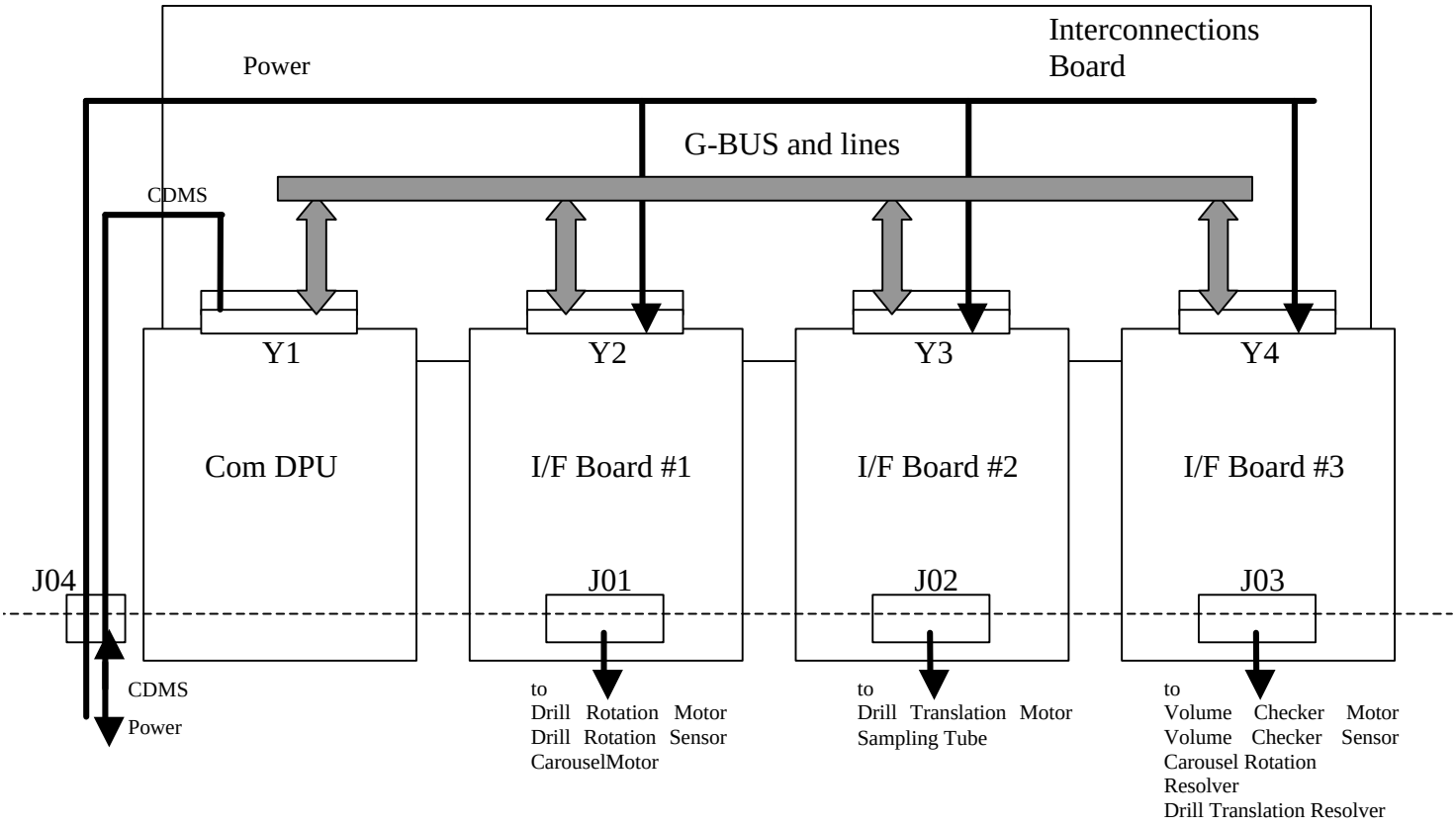


Fig. 2.5.1 SD2 external connections block diagram

SD2 Subsystem utilises the C-DPU. In Fig. 2.5.2 is reported the C-DPU block diagram (from RD3).

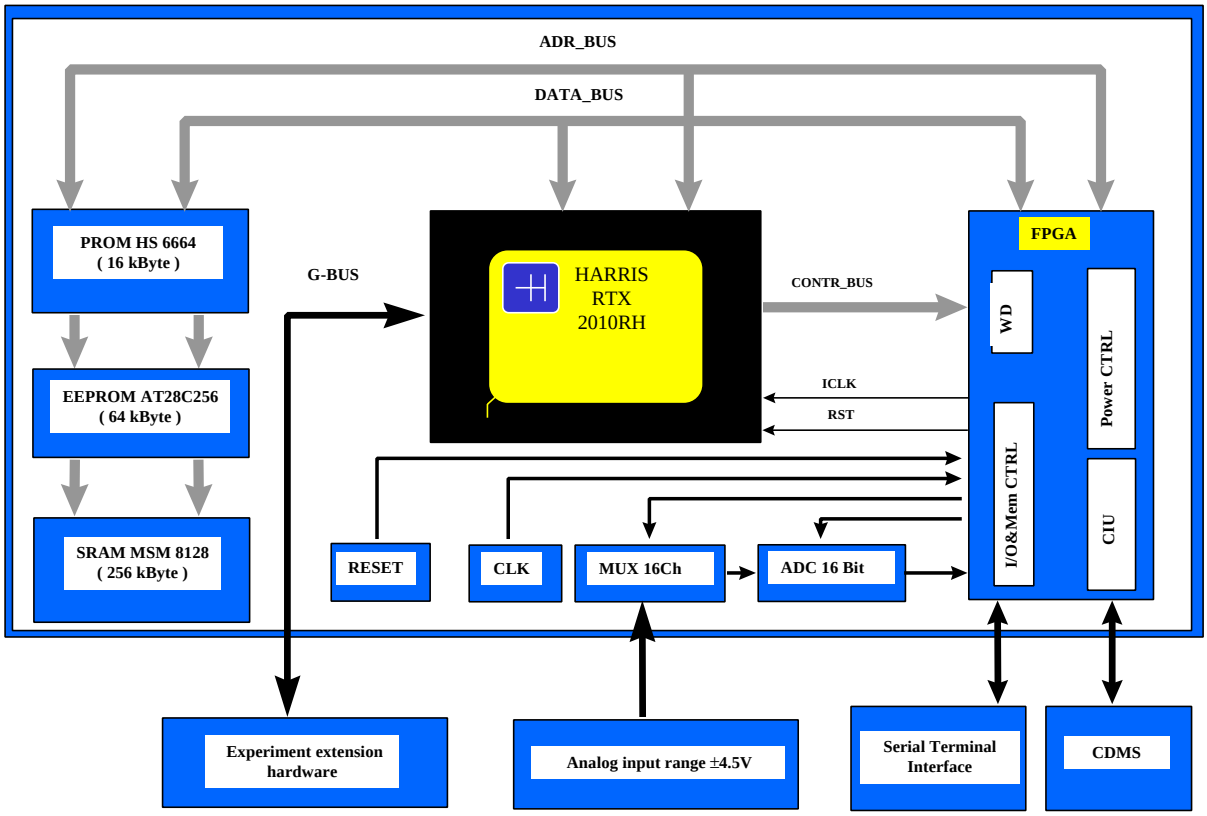


Fig. 2.5.2 C-DPU block diagram

The CDMS is connected with serial dedicated lines to the C-DPU.

The serial terminal interface (present only in the LM on a technological part extension) is provided only for software development and test.

The G-BUS is the parallel digital interface reserved to command and receive data to/from the dedicated interface boards to govern subsystem hardware devices (I/B Boards and relative motors, actuators, transducers).

Fifteen of the sixteen analog inputs (MUX 16 channels) are available to the I/F boards via G-BUS.

(Referring to RD3) Memory components are PROM (16 kByte), EEPROM (64 kByte) and static RAM (256 kByte).

The PROM is not implemented in the laboratory model. The EEPROM is replaced by ordinary EPROM.

At system reset the EPROM contents is copied by hardware into static RAM and then executed. Therefore the operating system uses a straight RAM model. System variables, interrupt tables, system software is allocated in RAM and can be changed and/or extended at run-time (or interactively).

3. SPECIFIC REQUIREMENTS

3.1 CAPABILITY REQUIREMENT

3.1.1 SD2 initialisation and operating modes

DELETED: SD2 works only in normal mode, not in stand-by

[UR-3.1.1-1] DELETED

[UR-3.1.1-2] DELETED

[UR-3.1.1-3] DELETED

[UR-3.1.1-4] DELETED

[UR-3.1.1-5] At power on the SD2_FSW shall start execution of the following activities:

- received command management. (ref. to chapter 3.1.2)
- internal time generation; (ref. to chapter 3.1.3)
- housekeeping and health check; (ref. to chapter 3.1.5)

3.1.2 CDMS communications

Data and command interchange between CDMS and SD2 occurs exclusively on word by word basis. A word is composed of 16 bits, MSB (bit15) first. (Ref. to AD1 for details).

According to [AD1], CDMS communicates with SD2 by sending the Subsystem Address Word (SSADR) and specifying the type of the command in the SSADR *Action Code* field. The Action Code list is specified in [AD1]. The commands specified in the Action Code field are called *Standard commands* and can be sent to SD2 and also to other Units.

When the Action Code is RCMD, then next sequence of Subsystem Command Word (SSCDM) sent by CDMS contains the data of a *Specific Command*, i.e. a command specific to SD2. The Specific Command list is reported in [AD1]. The Specific Commands are split into two types: *Immediate Specific Commands*, that shall be processed by SD2_FSW when received; *Normal Specific Commands*, executed when previous specific command execution is completed.

SD2_FSW shall provide the telemetry data: housekeeping data (HK_Data), scientific data (SC_Data), backup RAM data (RAM_Data), as specified in [AD1].

When SD2 requires to communicate with CDMS, it sets the Service Request Flag (SR) of Subsystem Status Word (SSTS) and sends the SSTS to CDMS. The type of request is specified in the *Request Code* field of Subsystem Data Word (SSDAT) transmitted back by SD2. The Request Code list is specified in [AD1].

According to the general concept that SD2 Subsystem is slave of CDMS and also considering possible criticisms of SD2 operation respect to power consumption and mechanical interaction, only simple consecutive execution of SD2 specific command is foreseen generally. Nevertheless a queuing mechanism is also possible.

[UR-3.1.2-1] The software shall:

- start the processing of *Standard Commands* (defined in [AD1]) as they are received;
- complete, as they are received, the processing the *Standard Commands* RTIM, TRQC, RHFM, THKD, TCMO, TSCR, TBUB, TBUF (see [AD1])
- queue the other *Standard Commands* in a RAM FIFO buffer whose dimension shall allow to store up to C_MAX_CDMS_MESSAGE *Standard Commands* and process them sequentially; if maximum buffer dimension is reached, the error shall be notified to Error Handler (ref. to error handler procedure, chapter 3.1.6)
- queue received SD2 *Specific Commands* (defined in [AD1]), in a RAM FIFO buffer whose dimension shall allow to store up to C_MAX_MP_WORDS words of specific telecommands coming from CDMS
- process the queued SD2 *Specific Commands* sequentially, each specific command is processed when the execution of the previous one is successfully completed

Note:

- the Standard Commands are executed under CDMS interrupt service routine (ISR), so that it is necessary to queue the Standard Commands whose time processing is greater than the processing time allowed by the CDMS ISR

- the execution of a specific command is completed when the target specified by the command has been reached; so, for a controlled position command, the specific command execution is completed when the target position has been reached and the motion is stopped, while for a speed controlled command, the command execution is completed when the target speed is reached even if the motion continues

[UR-3.1.2-2] SD2_FSW shall process the queued commands and delete them from the queue according to the order of reception.

[UR-3.1.2-3] DELETED

[UR-3.1.2-4] Exception to execution mechanism stated in requirement (UR-3.1.2-1,2) shall be provided only for Immediate specific command of SD2 Subsystem. When an Immediate specific command is received, it shall be executed immediately (ref. to chapter 3.2.1) even if another non immediate specific command is in execution.

Note:

In [AD1] it is reported the list of immediate/ normal specific commands.

[UR-3.1.2-5] When a command execution is started, a specific command replica is reported in the relevant SC_Data field as well as the command status (command-in-progress, command-failed, command-completed). When no specific command is in execution, the echo of last command is reported in SC_Data and the command status is either command-completed or command-failed.

Note:

The described mechanism allows to execute a list of consecutive specific command and it avoids possible not controlled concurrent execution of specific command interacting with hardware SD2 devices. Observing the telemetry data, subsequent SD2 specific operations may be monitored

3.1.2.1 Standard commands

For a general reference to each standard command refer to Rosetta Experiment Interface Document part A (HO-EST-RS-3002/EID-A ver. 5, chapter 3.3.5) (Ref. to AD1).

Operations of SD2_FSW, with respect to standard command received (Action Codes), are reported in the following.

[UR-3.1.2.1-1] Interface to CDMS shall be according to RD3.

[UR-3.1.2.1-2] Transmit request Code Word (TRQC)

Upon reception of this command, SD2_FSW shall provide a Request Code Word to CDMS.

Note:

This command is issued by CDMS whenever SD2_FSW set to '1' the Service Request flag in the SD2 Status Word, and is used for transmitting the Request Codes specified in [AD1].

[UR-3.1.2.1-3] Standby / Power Down Mode (STBY)

Upon reception of this command, an error flag shall be reported in to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.1-4] Receive Current CDMS Mode (RMOD)

Upon reception of this command, the SD2_FSW shall distinguish between CDMS normal mode and CDMS not normal mode (see [RD1]) and the CDMS mode shall be reported to Error Handler as error flag (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.1-5] Receive On-board Time (RTIM)

Upon this message SD2_FSW shall update the time in telemetry by using its internal time register. (Ref. to chapter 3.1.3)

Note This command is sent by CMDS, according to its current operational mode, in regular time intervals: every 1 second when CDMS is in normal mode; every 32 seconds when CDMS is in low power mode.

[UR-3.1.2.1-6] Receive Service System Status (RSST)

Upon reception of this command (Subsystem Address Word and Subsystem Command Words), the SD2_FSW shall distinguish between init-recovery-process and no-recovery-process. In any case, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.1-7] Deleted.

[UR-3.1.2.1-8] Receive Housekeeping Data Format Count (RHFM)

Upon reception of this command (Subsystem Address Word and Subsystem Command Word), SD2_FSW shall use the lower 4 bits of the associated Subsystem Command Word for selecting a HK data word source, which will then be acquired by CDMS by means of 'THKD' message. For HK data collection mechanism refer to [AD1-HouseKeeping Data].

[UR-3.1.2.1-9] Transmit Housekeeping Data Word (THKD)

Upon reception of this command, SD2_FSW shall deliver the HK data word identified by the current (previously received through RHFM) HK Data Format Count .

[UR-3.1.2.1-10] Receive Telecommand Sequence (RCMD)

This message will be used by CDMS to transmit to SD2 the SD2 specific commands.

Upon reception of this command (Subsystem Address Word and Subsystem Command Words), SD2_FSW shall handle the Subsystem Command Words as the command words relevant to a specific command.

[UR-3.1.2.1-11] Transmit Offset/Length of stored Telecommand Buffer Section (TCMO)

Upon reception of this command, SD2_FSW shall provide to CDMS the Offset and the Length (max 32 words) of Telecommand Buffer Section to be transferred from CDMS memory to SD2 internal buffer.

Note:

this command is used for loading a SD2 command sequence from CDMS memory to SD2 internal buffer. See [AD1- LDMP specific command communication protocol]

[UR-3.1.2.1-12] Receive Stored Telecommand Buffer Section (RCMS)

Upon reception of this command, SD2_FSW shall store the command words of RCMS into its internal buffer. The dimension of the buffer shall allow to store a whole mission plan consisting of C_MAX_MP_WORDS 16-bit words.

Note:

this command is used for loading a SD2 command sequence from CDMS memory to SD2 internal buffer. See [AD1- LDMP specific command communication protocol]

[UR-3.1.2.1-13] DELETED

[UR-3.1.2.1-14] Transmit Science data Burst (TSCR)

In response to this message SD2_FSW must send a HITB data burst to CDMS, according to [AD1- SD2 Scientific Data communication protocol]

[UR-3.1.2.1-15] DELETED

[UR-3.1.2.1-16] DELETED

[UR-3.1.2.1-17] Transmit pointer of Backup RAM Record (TBUP)

Upon reception of this command, SD2_FSW shall send to CDMS:

- either the address of backup RAM relevant to SD2 (SD2 Address and Pointer fields), according to [AD1-SD2 Backup RAM], when SD2_FSW requires CDMS to update the data relevant to SD2 backup RAM
- or the address of COSAC Backup RAM (according to [AD1- Backup-RAM of other Units]), for the acquisition of COSAC tapping station data
- or the address of PTOLEMY Backup RAM (according to [AD1- Backup-RAM of other Units]), for the acquisition of PTOLEMY tapping station data

- or the address of LANDING GEAR Backup RAM (according to [AD1- Backup-RAM of other Units]), for the acquisition of landing gear position

[UR-3.1.2.1-18] Transmit Backup RAM Record (TBUF)

Upon reception of this command, SD2_FSW shall send to CDMS the 32 words to be copied by CDMS in the backup RAM relevant to SD2, whose address has be sent by SD2_FSW by TBUP command.

[UR-3.1.2.1-19] Receive Backup RAM Record (RBUF)

Upon reception of this command (Subsystem Address Word and Subsystem Command Words), SD2_SW shall get in the 32 Subsystem Command Words the contents of the backup-RAM required by means of the 'Read Backup RAM Buffer Record' request code and TBUP command.

Note: RBUF will be received by SD2 after SD2 Service Request of COSAC and PTOLEMY backup-RAM contents for tapping stations status acquisition, or after SD2 Service Request of LANDING GEAR backup-RAM contents for landing gear position acquisition.

[UR-3.1.2.1-20] The SD2_FSW shall provide in Backup RAM the data specified in [AD1] (SD2 Current status, Actual Drill Depth, Carousel Position, Oven Number). The contents of BCK_Data shall be updated according to [AD1].

[UR-3.1.2.1-21] DELETED

[UR-3.1.2.1-22] DELETED

[UR-3.1.2.1-23] Receive Error Code Word (RERC)

Upon reception of this command, the SD2_FSW shall distinguish the kind of error code and report it to Error Handler as error flag (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.1-38] Retry-mechanism

When RERC is received, SD2_FSW shall re-start the communication protocol relevant to last non-completed request. The protocol shall restart up to C_CDMS_NUM_RETRY times.

[UR-3.1.2.1-35] When one of the following standard commands is received, a warning flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6):

RAXT

RASV

RSCS

RBUS

[UR-3.1.2.1-37] When one of the following standard commands is received,

TTRG

RTRG

the SD2_FSW shall ignore them: neither error flag in telemetry data, nor recovery action to be implemented.

[UR-3.1.2.1-36] When an Action Code different from the below specified is received, the SD2_SW shall rejects it, sets the ME flag of status word to '1', and an error flag shall be reported to HK_Data according to [AD1] (ref. to error handling procedure, chapter 3.1.6).

[UR-3.1.2.1-24] SD2_FSW shall set to "1" the SR flag in the Subsystem Status Word (SSTS, ref. to AD1 chapter 3.3.3) to signal to CDMS the necessity to communicate or transfer data.

Note

When SD2 has to communicate or transfer data to/from CDMS, it sets the SR flag in the SSTS. The CDMS replies with the TRQC message. SD2 replies back the Request Code (as Data Word), which specifies the reason of its request.

Operations of SD2_FSW, with respect to standard Request Code, are reported in the following.

[UR-3.1.2.1-25] DELETED

[UR-3.1.2.1-26] Send Stored Telecommand Buffer Section (SCMD)

SD2_FSW shall use this Request Code upon reception of specific command LDMP (see [AD1- LDMP specific command communication protocol]). This allows to start the load-command sequence protocol

[UR-3.1.2.1-27] DELETED

[UR-3.1.2.1-28] Science Data Ready (SRDY)

SD2_FSW shall use this Request Code to signal to CDMS that a Burst of HITB is ready to be transmitted (ref. to chapter 3.1.2.2.3 MHIT command)

[UR-3.1.2.1-29] DELETED

[UR-3.1.2.1-30] Write Backup RAM Record (WRBF)

This Request Code shall be used by SD2_FSW to notify CDMS that the BCK_Data record (32 BCK_Data) relevant to SD2 shall be updated by CDMS.

[UR-3.1.2.1-31] Read Backup RAM Record (RDBF)

This Request Code shall be used by SD2_FSW to notify CDMS that it is necessary to acquire Backup-RAM Record of other units

[UR-3.1.2.1-32] DELETED

[UR-3.1.2.1-33] Flush Last Science Data Packet (FLSP)

SD2_FSW shall use this Request Code after the complete dump of MHIT if the dimension of the whole dump is not an integer multiple of 128 words

[UR-3.1.2.1-34] Operation Completed (OCPL)

This Request Code shall be used by SD2_FSW to notify CDMS that a SD2 operation has been completed. (see AD1-STOPOP command)

3.1.2.2 Specific commands

According to specific SD2 operations, basic procedures and specific command shall be defined.

3.1.2.2.1 Basic procedures

External Mechanical Correctness

The following requirements [UR-3.1.2.2.1-17, 18, 19] specify the checks that SD2_FSW shall perform in order to verify if the mechanical conditions external to SD2 allow the motions

[UR-3.1.2.2.1-18] When a drill translation is commanded in the range [C_LANDG_MIN, C_LANDG_MAX] (as per Table B-1), SD2_FSW shall check if the mechanical conditions external to SD2 allow the drill translation without interference with landing gear legs. Drill translation in the range [C_LANDG_MIN, C_LANDG_MAX] is allowed only if the landing gear position is outside the forbidden ranges.

By default, when during the execution of this check no LANDG command has been received by SD2, the whole range [0,0xFFFF] shall be handled as forbidden range; this guarantees that it is not allowed the drill translation movement.

NOTE:

The landing gear position is retrieved via access to LANDING GEAR backup-Ram as specified in [AD1-Access to Backup RAM of other units], while the forbidden ranges are known via the parameters of LANDG command specified in [AD1]

[UR-3.1.2.2.1-19] When a carousel rotation is commanded, SD2_FSW shall check if mechanical conditions external to SD2 allow carousel rotation without interfering with capping stations. Carousel rotation is possible only when both COSAC and PTOLEMY capping stations are disengaged

NOTE:

the capping station status is retrieved via access to COSAC-Backup RAM and PTOLEMY-Backup RAM as specified in [AD1-Access to Backup RAM of other units].

[UR-3.1.2.2.1-20] If the commanded motion is not possible since the above specified checks fail, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

SD2 Mechanical Correctness

The following requirements [UR-3.1.2.2.1-1,2,3,16,13] specify the checks that SD2_FSW shall perform in order to verify if the SD2 mechanical conditions allow the motions.

[UR-3.1.2.2.1-1] When a drill translation is commanded, SD2_FSW shall check if the current drivers positions allow the drill translation. Drill translation is possible only:

in the sampling range C_SRDT when carousel is on its zero position with tolerance of C_ZECTO (as per Table B-1);

in the discharge range C_DRDT when one of the 26 ovens (# 1### 26) is correctly positioned under drill axis with tolerance of C_DOVTO (as per Table B-1);

in the re-arm range C_ARDT when the dummy oven (# 27) is correctly positioned under drill axis with tolerance of C_DDUTO (as per Table B-1)

in the default range C_DFDT in any other case

NOTE This check is not applicable to ZERO command. For the SD2 reference system, see [AD1].

[UR-3.1.2.2.1-2] When a carousel rotation is commanded, SD2_FSW shall check if Carousel rotation is possible. Carousel rotation is possible only when drill translation is on its zero position (i.e. it is less or equal to C_ZEDTO, as per Table B-1);

NOTE This check is not applicable to ZERO command. For the SD2 reference system, see [AD1].

[UR-3.1.2.2.1-3] When volume checker translation is commanded, SD2_FSW shall check if the volume checker translation is possible. Volume checker movement with direction 'DOWN' is possible only if one of 26 ovens is correctly positioned under its axis with tolerance of C_VOVTO, as per Table B-1, or when the zero carousel position is under its axis with tolerance C_ZECTO, as per Table B-1

NOTE This check is not applicable to ZERO and MVCK with direction 'UP' commands.

[UR-3.1.2.2.1-16] When a drill rotation is commanded, SD2_FSW shall check if drill rotation is possible. Drill rotation is possible only if the carousel is in its zero position with tolerance of C_ZECTO, as per Table B-1

[UR-3.1.2.2.1-17] When a sampling tube releasing is commanded, SD2_FSW shall check if the motion is possible. The motion is possible if either carousel is in zero position (with tolerance of C_ZECTO, as per Table B-1) or drill is in zero position (i.e. it is less or equal than C_ZEDTO, as per Table B-1)

[UR-3.1.2.2.1-11] If the commanded motion is not possible since the above specified checks fail, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6).

[**UR-3.1.2.2.1-4]** ***Minimum Path***

For carousel movement, according to initial and final position, SD2_FSW shall define the rotation direction to accomplish commanded movement with minimum rotation

[UR-3.1.2.2.1-5] ***Halt Procedure***

When it is required to perform a Halt Procedure, SD2_FSW shall verify if any movement is in course. If so, SD2_FSW shall perform a ramp down (ref. to Speed Control, UR-3.1.2.2.1-6 and 13) step-by-step movement to stop all motions and then switch-off relevant motor(s) power section(s) as defined by **[UR-3.1.2.2.2-2]**.

[UR-3.1.2.2.1-6] ***Speed Control of drill rotation***

When it is required the Speed Control of the drill rotation, SD2_FSW shall perform a speed ramp up/down procedure according to commanded target coasting speed and torque.

Speed ramping shall be executed according to the values in Appendix A.1 of [AD2], step by step, by means of successive speed commands, at the rate of C_MRFR Hz (as per Tab. B-1) (as per Table B-1).

The starting speed is:

a) the last commanded speed, read back from I/F boards, when the motor is moving;

b) zero, if the motor is still not commanded, halted or just switched off.

Note:

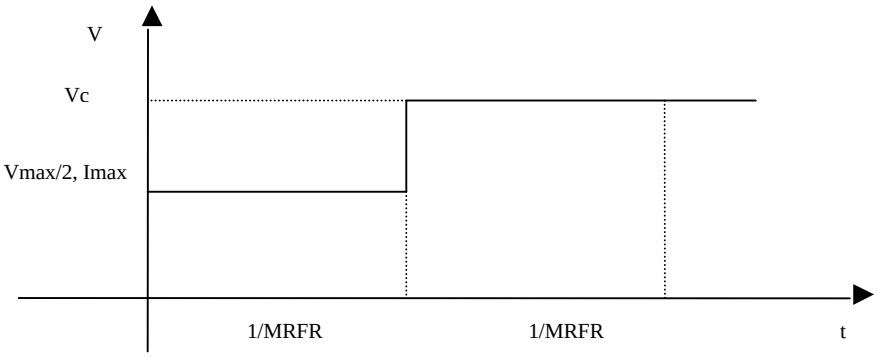
The Speed Control of drill rotation is required:

- either when the drill rotation command DRGO, is in execution
- or when the halt procedure is in execution, and the zero speed value is required

[UR-3.1.2.2.1-15] ***Speed Control of volume checker***

When it is required the speed control of volume checker, SD2_FSW shall perform the following, according to command type:

a) a MVCK UP/DOWN command is received. The SD2_FSW shall generate the speed commands according to the following:



first speed command: Vmax/2 and Torque value equal to Imax

next speed command: Vc (V commanded) and Torque value equal to commanded I

b) a halt command is received. The SD2_FSW shall perform a speed ramp down procedure starting from current one to speed zero. Speed ramping shall be executed according to the values in Appendix A.4 of [AD2], step by step by means of successive speed commands, at the rate of C_MRFR Hz (as per Tab. B-1) (as per Table B-1).

[UR-3.1.2.2.1-7] ***Position control*** (for drill translation and carousel rotation)

Position control for drill translation and carousel rotation shall be performed according to Annex A and according to commanded position, speed and torque.

[UR-3.1.2.2.1-8] DELETED

[UR-3.1.2.2.1-9] DELETED

[UR-3.1.2.2.1-10] ***Checksum***

When a specific command is received, SD2_FSW shall perform checksum calculation according to the following rule (possible overflow at any addition is always discarded):

$$\text{Checksum} = \#\#\# \sum_{n=1}^{m-1} \text{SSCMD}(n)$$

m is the number of words defining the specific command (checksum word excluded).

The evaluated checksum shall be compared with the word m of command: if they are not equal, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.2.1-12] ***Syntax Check***

When a specific command is processed, SD2_FSW shall check the contents of the command words with respect to the command specification in [AD1].

[UR-3.1.2.2.1-13] ***SD2 Current status.***

The SD2_FSW shall handle, according to [AD1], the following status:

- undefined status
- ready
- dead
- drill-in-progress
- drill-completed
- sampling-in-progress
- sampling-completed
- carousel-rotation-in-progress
- carousel-rotation-completed

When initialization is successfully completed, the status shall be "ready". When in "ready", the status is changed by successfully execution of specific commands STARTOP, STOPOP, ABRT, EMST, ENEM and by the recovery action executed by the error handler.

Note:

When in "undefined status", no activity is in progress: all devices are powered off, no speed-position control is in progress, no dump is in progress, no SD2 request to CDMS is in progress. When in undefined, the SD2 can be "safely" powered off.

Check command against SD2 status.

[UR-3.1.2.2.1-14.1] When SD2 status is *"dead"*, SD2_FSW shall reject any specific command with exception of ENEM, MHIT, STOPOP-SD2 Operation: an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.2.1-14.2] When SD2 status is "undefined", SD2_FSW shall reject any specific command with exception of STARTOP-SD2 Operation: an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.2.2.1-14.3] STOPOP-SD2 Operation shall be accepted only when all devices are powered-off.

[UR-3.1.2.2.1-14.4] Any specific command received during the execution of LDMP, i.e. during the loading of a mission plan, and different from ABRT and EMST shall be rejected: an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6). The loading of the mission plan shall anyway continue

[UR-3.1.2.2.1-14.5] A stored command sequence to be loaded by means of LDMP specific command shall not contain the following specific commands:

- LDMP
- ABRT
- EMST

If one of them is present, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6).

3.1.2.2.2 Specific simple commands

Operations of SD2_FSW, with respect to SD2 specific simple commands, are reported in the following (ref. to [AD1] for command format and data).

[UR-3.1.2.2.2-1] Perform zero condition and switch off all act. sections (ZERO)

Upon reception of this command, SD2_FSW shall position to "zero" the carousel rotation and drill translation. It shall perform the following operations.

- Execute Halt Procedure if a motion is in progress.
- Perform MVCK command with direction 'UP'
- Check that tapping stations are disengaged (verification via CDMS: SD2_FSW gets this data by accessing to COSAC/PTOLEMY Backup-RAM, according to [AD1]); if check fails an error flag shall be reported to HK_Data, according to [AD1] (ref. to error handling procedure, chapter 3.1.6).
- Switch on and set normal sections of drill translation resolver and carousel rotation resolver (as defined in **[UR-3.1.2.2.2-2])**
- Switch on power and set normal sections of drill translation motor and carousel rotation motors (as defined in **[UR-3.1.2.2.2-2])**
- Execute ACRE command to acquire drill position.

  ### If drill position < C_X_0 (as defined in Table B-1):

  - update drill depth in BCK_Data to 0xFFFF
  - perform position control of drill translation to zero position with C_ZERO_DT_SPEED speed and C_ZERO_DT_TORQUE torque
  - update drill depth in BCK_Data to "0"
  - update carousel position in BCK_Data to 0xFFFF (default value) and oven number to "undefined"
  - perform minimum path procedure for carousel;
  - perform position control of carousel rotation to zero position with C_ZERO_CAR_SPEED speed and C_ZERO_CAR_TORQUE torque
  - update carousel position in BCK_Data to "0" and oven number to "undefined"

  ### If drill position ### C_X_0 (as defined in Table B-1):

  - update carousel position in BCK_Data to 0xFFFF (default value) and oven number to "undefined"
  - perform minimum path procedure for carousel;
  - perform position control of carousel rotation to zero position with C_ZERO_CAR_SPEED speed and C_ZERO_CAR_TORQUE torque
  - update carousel position in BCK_Data to "0" and oven number to "undefined"
  - update drill depth in BCK_Data to 0xFFFF

- perform position control of drill translation to zero position with C_ZERO_DT_SPEED speed and C_ZERO_DT_TORQUE torque
- update drill depth in BCK_Data to "0"

- Switch off and set inhibit all actuation sections (as defined in **[UR-3.1.2.2.2-2])**

[UR-3.1.2.2.2-2] Switch On/Off electronic actuation sections (ONOF)

Upon this message SD2_FSW shall perform the following operations:

- Change the state of the actuation sections (Switch on/off) according to the command input data.
- Change of state of electronics power sections shall be performed in sequence with a pause between switching of any of two sections of at least C_SECTION_SWITCH_DELAY, as per Table B-1
- If the command requires switching ON of one of the motor driver electronics then it shall be performed in the following order:
  - set current setting of the motor to minimal value and speed to 0
  - wait C_SET_SPEED_DELAY, as per Table B-1
  - set the driver to inhibit state
  - switch on the actuator power section
  - wait C_POWER_SWITCH_DELAY, as per Table B-1
  - set the driver to normal state.
- If the command requires switching OFF of one of the motor driver electronics then it shall be performed in the following order:
  - set current setting of the motor to minimal value and speed to 0;
  - wait C_SET_SPEED_DELAY, as per Table B-1
  - set the driver to inhibit state;
  - switch off the actuator power section;
- If ONOF command requires to power on the sampling tube, the sampling tube shall be activated in continuous mode

Note:

When sampling tube is activated by means of ONOF command, it shall be powered off by means of ONOF- parameter B set to 0

[UR-3.1.2.2.2-3] Acquire values of drill translation resolver and/or carousel rotation resolver (ACRE)

Upon reception of this command, SD2_FSW shall perform the following operations:

- Switch on and set normal sections of drill translation resolver and/or carousel translation resolver (if not already active), according to the command input data (as defined in **[UR-3.1.2.2.2-2])**
- Wait for C_RESOLVER_POWER_DELAY (only if power sections have been just switched on)
- Perform acquisition of resolver data.

- Switch off and set inhibit sections of drill translation resolver and carousel translation resolver but only if they were not active at reception of ACRE. (as defined in **[UR-3.1.2.2.2-2])**

[UR-3.1.2.2.2-4] Perform carousel rotation to a defined position (CAPO)

Upon reception of this command, SD2_FSW shall perform the following operations.

1. Perform MVCU command with C_VCAC_TORQUE and C_VCAC_SPEED values
2. Perform ACRE command
3. Execute "SD2 Mechanical Correctness" and "External Mechanical Correctness" procedures relevant to carousel and "Minimum Path" procedures.
4. Update carousel position in BCK_Data to 0xFFFF (default value) and oven number to "undefined"
5. Switch on and set normal sections of carousel resolver and carousel motor (as defined in **[UR-3.1.2.2.2-2])**
6. Perform Position Control of carousel to defined position
7. Switch off and set inhibit sections of carousel resolver and carousel motor (as defined in **[UR-3.1.2.2.2-2])**
8. Update carousel position in BCK_Data to the defined position and the oven number to "undefined", according to [AD1]

[UR-3.1.2.2.2-5] Perform car. rot. to move an oven to a scientific port (CASI)

Upon reception of this command, SD2_FSW shall perform the following operations.

- Evaluate the target position according to scientific port number and oven number (ref. to [AD1])
- Perform CAPO command, items 1 ..7
- Update carousel position in BCK_Data to the defined position and the oven number to defined one, according to [AD1]

[UR-3.1.2.2.2-6] Perform drill translation to a defined position (DRTR)

Upon reception of this command, SD2_FSW shall perform the following operations.

- Perform ACRE command
- Execute "SD2 Mechanical Correctness" and "External Mechanical Correctness" procedures relevant to drill translation.
- Update drill depth in BCK_Data to 0xFFFF (default value)
- Switch on and set normal sections of drill translation resolver and drill translation motor (as defined in **[UR-3.1.2.2.2-2])**
- Perform Position Control of drill translation to the defined position
- Switch off and set inhibit sections of drill translation resolver and drill translation motor (as defined in **[UR-3.1.2.2.2-2])**

- Update “Drill Depth" of BCK_Data to the defined position, according to [AD1]

[UR-3.1.2.2.2-7] Perform drill rotation for a defined time (DRGO)

Upon reception of this command, SD2_FSW shall perform the following operations.

- Execute “SD2 Mechanical Correctness” procedure relevant to drill rotation
- Switch on and set normal sections of drill rotation motor, with motion direction according to the commanded one (as defined in **[UR-3.1.2.2.2-2])**
- Perform speed control of drill rotation
- Activate drill rotation periodic check (see UR-3.1.5-5) with commanded speed as reference speed.

[UR-3.1.2.2.2-8] Perform drill rotation stop (DRST)

Upon reception of this command, SD2_FSW shall perform the following operations.

- Deactivate drill rotation periodic check (see UR-3.1.5-5)
- Perform speed control down to zero coasting speed, with the actual value of torque.
- Switch off and set inhibit section of drill rotation motor (as defined in **[UR-3.1.2.2.2-2])**

[UR-3.1.2.2.2-9] Perform drill rotation stop after a defined time (time-out)

After having received a DRGO command, a drill rotation stop (DRST) shall be performed when the specified time is elapsed.

[UR-3.1.2.2.2-10] DELETED

[UR-3.1.2.2.2-11] DELETED

[UR-3.1.2.2.2-12] DELETED

[UR-3.1.2.2.2-13] Move Volume Checker Up

Upon reception of MVCK with direction ‘UP’, SD2_FSW shall perform the following operations.

1) Perform switch on and set normal sections of volume checker section, with motion direction ‘Up’ (as defined in **[UR-3.1.2.2.2-2])**
2) Check if upper microswitch is already reached: if so, power off the volume checker motor and go to step 7
3) Reset and start volume checker counter
4) Perform speed control of volume checker
5) Start the timer

6) Every C_VOLCHK_SWITCH_PERIOD check if volume checker upper microswitch is on;

- if volume checker upper microswitch is on, power off the volume checker motor in order to stop the counting (as defined in **[UR-3.1.2.2.2-2])**

- if volume checker upper microswitch is not on and the time is elapsed (i.e. the time from begin of step 4 up to now is greater than the timeout specified by the command), repeat steps 5 and 6. If the check fails again, power off the volume checker motor (as defined in **[UR-3.1.2.2.2-2])** and report an error flag to Error Handler (ref. to error handling procedure, chapter 3.1.6)

7) Read volume checker counter and store Volume Checker Displacement to word named VCD of SC_Data, according to [AD1]

8) Stop all sections of volume checker (as defined in **[UR-3.1.2.2.2-2])**

[UR-3.1.2.2.2-14] Move Volume Checker Down

Upon reception of MVCK with direction 'DOWN', SD2_FSW shall perform the following operations.

1) Perform ACRE to acquire carousel position
2) Execute "SD2 Mechanical Correctness" procedure relevant to volume checker.
3) Perform switch on and set normal sections of volume checker section, with motion direction 'Down' (as defined in **[UR-3.1.2.2.2-2])**
4) Reset and start volume checker counter
5) Perform speed control of volume checker
6) Wait for timeout specified in the command
7) Read volume checker counter
8) Stop volume checker motor (as defined in **[UR-3.1.2.2.2-2])**, store volume checker counter into word named VCD of SC_Data, according to [AD1]
9) Switch off all volume checker section (as defined in **[UR-3.1.2.2.2-2])**

[UR-3.1.2.2.2-15] Perform volume checker activation (VCAC)

Upon this message SD2_FSW shall perform the following operations.

- Perform MVCK with C_VCAC_TORQUE and C_VCAC_SPEED values, direction UP and timeout specified in the command
- Copy SC_data VCD into VC1
- Perform MVCK with commanded torque-speed values with direction DOWN and timeout specified in the command
- Copy SC_data VCD into VC2
- Wait for the time specified in the command
- Perform MVCK with C_VCAC_TORQUE and C_VCAC_SPEED values, direction UP and timeout specified in the command

- Copy SC_data VCD into VC3

[UR-3.1.2.2.2-16] DELETED

[UR-3.1.2.2.2-17] DELETED

[UR-3.1.2.2.2-18] DELETED

[UR-3.1.2.2.2-19] DELETED

[UR-3.1.2.2.2-20] DELETED

[UR-3.1.2.2.2-21] Abort Command (ABRT)

Upon reception of command, SD2_FSW shall perform the following operations.

- Execute the Halt procedure.
- Switch off and set inhibit all the motors, resolvers, sensors power sections (as defined in **[UR-3.1.2.2.2-2])**.
- Terminate execution of the current command.
- remove all the specific commands pending in the command queue
- abort the loading of a command sequence (LDMP), if any
- enter in “dead status” and update the telemetry data relevant to SD2 status

[UR-3.1.2.2.2-22] Emergency Stop (EMST)

Upon reception of command, SD2_FSW shall perform the following operations.

- Switch off and set inhibit all the motors, resolvers, sensors power sections (as defined in **[UR-3.1.2.2.2-2])**.
- Terminate execution of the current command.
- remove all the specific commands pending in the command queue
- abort the loading of a command sequence (LDMP), if any
- enter in “dead status” and update the telemetry data relevant to SD2 status

[UR-3.1.2.2.2-23] Enable/disable error handling procedure (EHEN)

Upon reception of command, SD2_FSW shall enable/disable the error handling procedure (ref. to chapter 3.1.6) according to the command parameters, and update the word named EHSTATUS of telemetry data according to [AD1].

[UR-3.1.2.2.2-24] Release sampling tube (SARE)

Upon reception of command, SD2_FSW shall perform the following operations:

- Perform ACRE command to acquire carousel and drill positions
- Execute "SD2 Mechanical Correctness" procedure relevant to sampling tube
- Activate the sampling tube activation mode by means of a fixed duration current pulse of 50 ms

[UR-3.1.2.2.2-25] Read the contents of the specified board address (RDAD)

Upon reception of command, SD2_FSW shall perform the following operations:

- Acquire the contents of the specified board address and store it into the word named ADRVAL of SC_Data, according to [AD1]
- Store into the word named MEMADR of SC_Data the specified board address, according to [AD1]

[UR-3.1.2.2.2-26] Write the specified word into the specified board address (WRAD)

Upon reception of command, SD2_FSW shall perform the following operations:

- Write the specified word into the specified board address

[UR-3.1.2.2.2-27] End of emergency (ENEM)

Upon reception of command, SD2_FSW shall perform the following operations:

- changes the SD2 current status from "dead" to "ready", allowing SD2_FSW to accept and execute new commands
- update the telemetry data relevant to SD2 status
- clear the error condition in telemetry data

Note:

When in emergency status, SD2_FSW shall accept only ENEM, MHIT and STOPOP-SD2 Operation commands

[UR-3.1.2.2.2-28] LDMP (Load Command Sequence)

Upon reception of command, SD2_FSW shall perform the following operations:

- starts the loading of the telecommand buffer section stored into CDMS memory: blocks of 32 words shall be loaded from CDMS memory into SD2 internal buffer according to the protocol specified in [AD1], until the whole command sequence (whose length is specified in the command) has been loaded; the last block will be the remainder of command sequence length split into blocks of 32 words
- when the loading is completed, SD2_FSW shall evaluate the command sequence checksum according to Adler32 algorithm and shall compare it with the expected checksum provided by the LDMP command; if check fails, an error flag shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6), the internal buffer

containing the command sequence shall be flushed and SD2_FSW shall start the whole command sequence loading again. The re-loading can be repeat up to C_LOAD_MAX_NUM times.

- when the loading is successfully completed, SD2_FSW shall start the processing of the specific commands contained in it, in FIFO order

Note:

during command sequence loading, any specific commands different from ABRT and EMST shall be rejected and an error flag shall be reported to HK_Data according to [AD1] (ref. to error handling procedure, chapter 3.1.6).

[**UR-3.1.2.2.2-29]** STARTOP (Start drilling/ sampling operation)

Upon reception of command, SD2_FSW shall set the SD2_Current_Status of telemetry data with (see [AD1]):

- drill in progress, if the command parameter OP is drill
- sampling in progress, if the command parameter OP is sampling
- carousel rotation in progress, if the command parameter OP is carousel rotation
- SD2, if the command parameter is SD2-Operation

[UR-3.1.2.2.2-30] STOPOP (Stop drilling/ sampling operation)

Upon reception of command, SD2_FSW shall set the SD2_Current_Status of telemetry data with (see [AD1]):

- drill completed, if the command parameter OP is drill
- sampling completed, if the command parameter OP is sampling
- carousel rotation completed, if the command parameter OP is carousel rotation
- undefined, if the command parameter is SD2 Operation.

Moreover, if NOTIFY field holds ‘1’, the CDMS shall be notified that an operation has been completed (via SR flag and OCPL Request Code)

[UR-3.1.2.2.2-31] DELAY

Upon reception of command, SD2_FSW shall wait for the specified time before to execute next specific command

[UR-3.1.2.2.2-32] LANDG

Upon reception of command, SD2_FSW shall get from the command parameters the “word_index” and the forbidden ranges to be used for the execution of “External Mechanical Correctness” procedure relevant to drill translation motion.

[UR-3.1.2.2.2-33] DRTT- drill translation with timeout

Upon reception of this command, SD2_FSW shall perform the following operations.

- Perform ACRE command
- Execute “SD2 Mechanical Correctness” and “External Mechanical Correctness” procedures relevant to drill translation.
- Update drill depth in BCK_Data to 0xFFFF (default value)
- Switch on and set normal sections of drill translation resolver and drill translation motor (as defined in **[UR-3.1.2.2.2-2])**
- Perform Position Control of drill translation to the defined position: the motion shall be declared completed either because the target position has been reached, or because the time is elapsed. During the movement, the drill translation speed periodic check specified in [UR-3.1.5-10] shall not be performed.
- Switch off and set inhibit sections of drill translation resolver and drill translation motor (as defined in **[UR-3.1.2.2.2-2])**
- Update “Drill Depth" of BCK_Data to the defined position, according to [AD1]

[UR-3.1.2.2.2-34] DRTC- drill translation check

Upon reception of this command, SD2_FSW shall perform the following operations.

- Perform ACRE command
- Execute “SD2 Mechanical Correctness” and “External Mechanical Correctness” procedures relevant to drill translation.
- Update drill depth in BCK_Data to 0xFFFF (default value)
- Switch on and set normal sections of drill translation resolver and drill translation motor, either main or redundant windings according to input parameter (as defined in **[UR-3.1.2.2.2-2])**
- Perform Position Control of drill translation to the defined position. If the time specified in the command elapses, the check failure main-motion-check-failure or redundant-motion-check-failure shall be raised. During the movement, the drill translation speed periodic check specified in [UR-3.1.5-10] shall not be performed.
- Switch off and set inhibit sections of drill translation resolver and drill translation motor (as defined in **[UR-3.1.2.2.2-2])**
- Update “Drill Depth" of BCK_Data to the defined position, according to [AD1]

Upon reception of command, SD2_FSW shall get from the command parameters the “word_index” and the forbidden ranges to be used for the execution of “External Mechanical Correctness” procedure relevant to drill translation motion.

3.1.2.2.3 Specific composite commands

DELETED. All specific commands are simple.

[UR-3.1.2.2.3-1] DELETED

[UR-3.1.2.2.3-2] DELETED

[UR-3.1.2.2.3-3] DELETED

[UR-3.1.2.2.3-4] DELETED

[UR-3.1.2.2.3-5] DELETED

[UR-3.1.2.2.3-6] DELETED

Managing HITB acquisition (MHIT)

The HITB (Historical Internal Tracking Buffer) facility may be activated by CDMS, in parallel with normal housekeeping data management. In this way it is possible to save interesting SD2 internal data. HITB may be useful to reconstruct in details the operations of SD2 Subsystem.

This data buffer of SD2 will be handled by CDMS as scientific data.

[UR-3.1.2.2.3-7] SD2_FSW shall allocate to HIBT enough RAM memory to store C_SC_DATE_NUM_FRAMES number of Scientific Data frames. The buffer shall be handled as circular buffer.

[**UR-3.1.2.2.3-8]** At initialisation, SD2_FSW shall autonomously start HITB acquisition data according to [AD1]:

- The SC_Data words are copied in consecutive locations of HITB every C_HITB_DEF_ACQ

Upon reception of MHIT command, SD2_FSW (according to S/H field) shall operate as reported in the following.

[UR-3.1.2.2.3-9] If S/H bit is set, SD2_FSW shall modify acquisition rate of HITB data according to the rate specified in the command field ACQ.Period.

[UR-3.1.2.2.3-10] If S/H bit is reset, SD2_FSW shall stop acquisition of HITB and it shall signal to CDMS that SC_Data are ready to be transferred, according to [AD1].

[UR-3.1.2.2.3-11] The HITB dump shall be continued (according to the transfer protocol to CDMS) up to all HITB data are transferred to CDMS.

[UR-3.1.2.2.3-12] After completion of HITB dump, HITB acquisition shall be restarted.

[UR-3.1.2.2.3-13] Deleted

3.1.3 Timing

[UR-3.1.3-1] To support time depending actions, SD2_FSW shall maintain an internal timing, starting from zero at power up

[UR-3.1.3-2] When the RTIM message form CDMS is received, the two words related to RTIM shall be reported into SC_Data according to [AD1] updated by means of internal timing.

Note:

RTIM is received every about 1 [s]. The time when the RTIM is written in telemetry data depends on SD2_FSW telemetry scheduling. The RTIM and the telemetry are not syncronized, so that it is necessary to report the value of RTIM updated by means of the internal timing.

3.1.4 I/F Board operations

SD2_FSW interfaces the SD2 I/F boards by means of a couple of bi-directional register (16 bit wide). The 4 registers are: DATAIN (data input register), DATAOUT (data output register), CONTROL (control input register) and STATUS (status output register). The first two are reserved for data interchange; the second two for command reception and for status presentation. These registers are viewed by the SD2_FSW as I/O registers on the G-BUS addressing space. To perform message synchronisation two bits of STATUS register are used as flag bits. Refer to AD2 for details.

[UR-3.1.4-1] For each I/F boards, SD2_FSW shall implement an I/F procedure, according to AD2, to transfer data to/from the board to operate SD2 devices, and to read back the I/F Board status to verify the correctness of board operation.

[UR-3.1.4-2] DELETED

3.1.5 Status data and health check management

SD2_FSW provides, as telemetry data:

- housekeeping data (HK_Data)
- scientific data (SC_Data)
- backup RAM data (BCK_Data)

They are listed in [AD1].

[UR-3.1.5-1] The SD2_FSW shall provide the HK_Data specified in [AD1], according to the protocol specified in [AD1].

[**UR-3.1.5-2]** The SD2_FSW shall provide the SC_Data specified in [AD1], according to the protocol specified in [AD1]

[**UR-3.1.5-8]** The SD2_FSW shall provide the BCK_Data specified in [AD1], according to the protocol specified in [AD1]

[UR-3.1.5-3] DELETED

[UR-3.1.5-4] DELETED

[UR-3.1.5-5] Drill rotation periodic check.

When the Drill rotation periodic check is activated with coasting speed Vc and Vc is greater than C_CHK_DR_MIN_SPEED, then the drill rotation check shall be executed: the SD2_FSW shall acquire every C_CHK_DR_PERIOD the data out # 1 register of I/F board #1 (rotation detector data RDD), compute drill speed as

Ds = RDD/C_NUM_PULSE_PER_ROUND /C_CHK_DR_PERIOD

copy Ds into RODRI word of SC_Data, according to [AD1], check that

###Ds-Vc### < C_CHK_DR_SPEED_TOL;

if it is not so (i.e. |Ds-Vc| > C_CHK_DR_SPEED_TOL), then the error shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6)

[UR-3.1.5-6] Speed error check. DELETED

[UR-3.1.5-7] Drill translation redundancy check. DELETED

[UR-3.1.5-9] DELETED

[UR-3.1.5-10] Drill translation speed periodic check

When position control of drill translation is active, the acceleration ramp is completed and the coasting speed Vc is greater than C_CHK_DT_MIN_SPEED, then the drill translation speed check shall be executed: the SD2_FSW shall acquire every C_CHK_DT_PERIOD the drill position, evaluate the current drill translation speed Vm

Vm = |Current_Drill_Pos – Previous_Drill_Pos| / C_CHK_DT_PERIOD

then check that

|Vm –Vc | / Vc <= C_CHK_DT_SPEED_TOL

If it is not so (i.e. |Vm – Vc| / Vc > C_CHK_DT_SPEED_TOL), then the error shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6).

[UR-3.1.5-11] Carousel speed periodic check

When position control of carousel is active, the acceleration ramp is completed and the coasting speed Vc is greater than C_CHK_CAR_MIN_SPEED, then the carousel speed check shall be executed: the SD2_FSW shall acquire every C_CHK_CAR_PERIOD the carousel position, evaluate the current carousel speed Vm

Vm = |Current_Carousel_Pos – Previous_Carousel_Pos| / C_CHK_CAR_PERIOD

then check that

|Vm –Vc | / Vc <= C_CHK_CAR_SPEED_TOL

If it is not so (i.e. |Vm – Vc| / Vc > C_CHK_CAR_SPEED_TOL), then the error shall be reported to Error Handler (ref. to error handling procedure, chapter 3.1.6).

[UR-3.1.5-12] SD2_FSW – CDMS communication protocol timeout

SD2_FSW shall implement a timeout mechanism when it starts a communication protocol with CDMS. If the communication is not successfully completed within C_CDMS_TIMEOUT time, an error flag shall be sent to Error Handler as warning and the communication protocol re-starts again. If the communication protocol fails after C_CDMS_NUM_RETRY, the relevant selectable error shall be sent to Error Handler (ref. to error handling procedure, chapter 3.1.6).

Note:

this check allows to avoid SD2 deadlock when communication with CDMS is not OK.

3.1.6 Error handling

According to slave concept of SD2 Subsystem and to its possible critic operations, the only recovery actions performed by SD2_FSW will be:

- either execute all the actions foreseen for EMST command
- or execute all the actions foreseen for ABRT command
- or activate redundant winding of drill translation

[UR-3.1.6-1] SD2_FSW shall manage an Error Handling procedure, which shall be waiting for errors whose severity, according to [AD1], can be:

- ignore
- warning
- drill_translation_check
- soft emergency selectable
- soft emergency always selected
- hard emergency selectable
- hard emergency always selected

[UR-3.1.6-2] SD2_FSW shall manage an Error Handling procedure, which shall be waiting for any hard emergency error condition, either selectable or always selected. When a hard emergency error is detected, the following recovery procedure shall be executed:

- the relevant ERFG shall be reported in telemetry data according to [AD1]
- the actions relevant to EMST command shall be executed. As a consequence, SD2 enters in Dead status.

[UR-3.1.6-3] When the drill translation speed check error (ref. to UR-3.1.5-7) is detected, the relevant ERFG shall be reported in telemetry data according to [AD1] and the following recovery procedure shall be applied:

- continue the drill translation but use as torque C_DT_RECOVERY_TORQUE
- if the check fails again, continue the drill translation by using C_DT_RECOVERY_TORQUE and by powering both main and redundant drivers
- if the check fails again, the actions relevant to ABRT command shall be executed. As a consequence, SD2 enters in Dead status
- at start of each drill translation motion, no recovery procedure shall be executed (i.e., each drill translation motion shall start by powering only main winding and by using the torque specified in the relevant specific command)

NOTE At initialisation the main winding is selected.

[UR-3.1.6-4] Deleted

[UR-3.1.6-5] When a “warning” error condition is detected, it shall be reported in telemetry data according to [AD1] and no other action shall be performed.

[UR-3.1.6-6] When an “ignore” error condition is detected, it shall not be reported in telemetry data and no recovery action shall be executed: the error condition is ignored and SD2_FSW continues its processing

[UR-3.1.6-7] SD2_FSW shall manage an Error Handling procedure, which shall be waiting for any soft emergency error condition, either selectable or always selected. When a soft emergency error is detected, the following recovery procedure shall be executed:

- the relevant ERFG shall be reported in telemetry data according to [AD1]
- the actions relevant to ABRT command shall be executed. As a consequence, SD2 enters in Dead status.

[UR-3.1.6-8] When a selectable error is detected (either soft or hard) and the relevant recovery action is disabled by the EHEN command, the detected error shall be reported in telemetry data and SD2_FSW shall continue its processing

[UR-3.1.6-9] Only the following recovery actions can be disabled by the EHEN:

- recovery actions related to CDMS communication errors
- recovery actions related to backup RAM read/write request errors
- recovery actions related to contents of COSAC/ PTOLEMY/ LANDG backup RAM contents
- recovery actions related to "drill_translation-check"

Note:

The recovery actions that can be disabled by EHEN specific command are relevant to errors whose severity is either “drill_translation_check”, or “soft emergency selectable”, “hard emergency selectable”

3.2 CONSTRAINT REQUIREMENTS

3.2.1 Timing

[UR-3.2.1-1] DELETED

[UR-3.2.1-2] Deleted.

[UR-3.2.1-3] DELETED

[UR-3.2.1-4] DELETED

[UR-3.2.1-5] Immediate specific command shall be executed within (cdms_num_message +1) * C_COMMAND_PERIOD with respect to the moment of reception of full command packet.

cdms_num_message is the number of CDMS messages sent by CDMS and not yet processed, and its range is [0, C_MAX_CDMS_MESSAGE].

Note:

- the execution of immediate specific commands depends on the number cdms_num_message of CDMS messages present in the CDMS message queue.
- The worst case for the immediate command execution happens when the CDMS message queue is full, and this means that C_MAX_CDMS_MESSAGE number of specific commands sent by CDMS are received by SD2 within just one C_COMMAND_PERIOD.
- In the flight ROSETTA scenario, the nominal SD2 mission will be performed via a stored command sequence loaded by means of LDMP specific command. In this case, the CDMS message queue will contain only the LDMP command so that the execution of immediate specific command will required:
  - 2* C_COMMAND_PERIOD if the immediate specific command is sent by CDMS less than C_COMMAND_PERIOD after the LDMP command
  - 1* C_COMMAND_PERIOD in any other case

3.2.2 Maintainability

None

3.2.3 Safety

Based on “Product Assurance Plan for SHARK program”, SHARK-QA-TS-005, no part of SD2_FSW is safety critical.

3.2.4 Resource

[UR-3.2.4-1] Software related resources shall take into account the following C-DPU hardware features.

EEPROM 64 kByte

3.2.5 Verification

Referring to AD3, all software verification and validation activities shall be documented in Software Verification and Validation Plan (SVVP).

[UR-3.2.5-1] The SD2_FSW system and acceptance test shall be performed on the following environment:

- SD2 Electronic EQM or FM or FS Unit, which is representative of flight HW as far as SW aspects are concerned
- CDMS Simulator shall be used for CDMS-SD2_FSW communication
- Mechanical equipment EGSE-1 specified in [RD2]

The unit and integration tests which will require a printable output will be performed on the LM CommonDPU or in the following test environment:

- SGSE-1, the software ground support equipment consisting of the three EM boards specified in [RD5] and the LM CommonDPU

4. TRACEABILITY MATRIX

4.1 TRACEABILITY FROM URD TO SPECIFICATION REQUIREMENTS

For each requirement stated herein before, a reference to specifications requirements defined in [AD4] is reported in the following table.

User Requirement ID	Specification Id
3.1.1-01	DELETED
3.1.1-02	DELETED
3.1.1-03	DELETED
3.1.1-04	DELETED
3.1.1-05	4.4.2-01
3.1.2-01	4.2.2-01
3.1.2-01	2.1-05
3.1.2-01	4.2.3-02
3.1.2-02	4.2.3-04
3.1.2-03	DELETED
3.1.2-04	4.2.3-05
3.1.2-05	4.2.4-01
3.1.2.1-01	4.2.3-01
3.1.2.1-02	4.2.2-01
3.1.2.1-03	4.2.2-02
3.1.2.1-04	4.2.2-02
3.1.2.1-05	4.2.2-01
3.1.2.1-06	4.2.2-02
3.1.2.1-07	DELETED
3.1.2.1-08	4.2.2-01
3.1.2.1-09	4.2.2-02
3.1.2.1-10	4.2.2-01
3.1.2.1-11	4.2.2-01
3.1.2.1-12	4.2.2-01
3.1.2.1-13	DELETED
3.1.2.1-14	4.2.2-01
3.1.2.1-15	DELETED
3.1.2.1-16	DELETED
3.1.2.1-17	4.2.2-01
3.1.2.1-18	4.2.2-01
3.1.2.1-19	4.2.2-01
3.1.2.1-20	4.2.4-03
3.1.2.1-21	DELETED
3.1.2.1-22	DELETED
3.1.2.1-23	4.2.2-02

3.1.2.1-24	4.2.1-01
3.1.2.1-25	DELETED
3.1.2.1-26	4.2.2-01
3.1.2.1-27	DELETED
3.1.2.1-28	4.2.2-01
3.1.2.1-29	DELETED
3.1.2.1-30	4.2.2-01
3.1.2.1-31	4.2.2-01
3.1.2.1-32	DELETED
3.1.2.1-33	4.2.2-01
3.1.2.1-34	4.2.2-03
3.1.2.1-35	4.2.2-02
3.1.2.1-36	4.2.3-06
3.1.2.1-37	4.2.2-02
3.1.2.1-38	4.2.3-06
3.1.2.2.1-01	2.2-01
3.1.2.2.1-02	2.2-01
3.1.2.2.1-03	2.2-01
3.1.2.2.1-04	2.1-01
3.1.2.2.1-05	2.1-09
3.1.2.2.1-06	2.1-04
3.1.2.2.1-07	2.1-01
3.1.2.2.1-07	2.1-03
3.1.2.2.1-07	3.3.5
3.1.2.2.1-08	DELETED
3.1.2.2.1-09	DELETED
3.1.2.2.1-10	4.2.3-02
3.1.2.2.1-11	2.3-01
3.1.2.2.1-12	4.2.3-02
3.1.2.2.1-13	4.2.3-02
3.1.2.2.1-14.1	4.2.3-02
3.1.2.2.1-14.1	2.1-10
3.1.2.2.1-14.2	4.2.3-02
3.1.2.2.1-14.3	4.2.3-02
3.1.2.2.1-14.4	4.2.3-02
3.1.2.2.1-14.5	4.2.3-02
3.1.2.2.1-15	2.1-06
3.1.2.2.1-16	4.2.2-01
3.1.2.2.1-17	4.2.2-01
3.1.2.2.1-18	2.2-02
3.1.2.2.1-19	2.2-02
3.1.2.2.1-20	2.3-01
3.1.2.2.2-01	4.2.3-03
3.1.2.2.2-02	4.2.3-03
3.1.2.2.2-03	4.2.3-03

3.1.2.2.2-03	2.1-11
3.1.2.2.2-04	4.2.3-03
3.1.2.2.2-04	2.1-01
3.1.2.2.2-04	2.1-11
3.1.2.2.2-05	4.2.3-03
3.1.2.2.2-05	2.1-02
3.1.2.2.2-06	4.2.3-03
3.1.2.2.2-06	2.1-03
3.1.2.2.2-06	2.1-11
3.1.2.2.2-06	2.4.3.2
3.1.2.2.2-07	4.2.3-03
3.1.2.2.2-07	2.1-04
3.1.2.2.2-07	2.1-11
3.1.2.2.2-08	2.1-11
3.1.2.2.2-08	4.2.3-03
3.1.2.2.2-09	4.2.3-03
3.1.2.2.2-10	DELETED
3.1.2.2.2-11	DELETED
3.1.2.2.2-12	DELETED
3.1.2.2.2-13	4.2.3-03
3.1.2.2.2-13	2.1-11
3.1.2.2.2-13	2.1-06
3.1.2.2.2-14	4.2.3-03
3.1.2.2.2-14	2.1-06
3.1.2.2.2-14	2.1-11
3.1.2.2.2-15	4.2.3-03
3.1.2.2.2-15	2.1-06
3.1.2.2.2-16	DELETED
3.1.2.2.2-17	DELETED
3.1.2.2.2-18	DELETED
3.1.2.2.2-19	DELETED
3.1.2.2.2-20	DELETED
3.1.2.2.2-21	4.2.3-03
3.1.2.2.2-21	2.1-09
3.1.2.2.2-22	4.2.3-03
3.1.2.2.2-22	2.1-09
3.1.2.2.2-23	2.3-04
3.1.2.2.2-23	2.3-05
3.1.2.2.2-23	4.2.3-07
3.1.2.2.2-24	4.2.3-03
3.1.2.2.2-24	2.1-07
3.1.2.2.2-24	2.1-11
3.1.2.2.2-25	4.2.3-02
3.1.2.2.2-26	4.2.3-02
3.1.2.2.2-27	4.2.3-02

3.1.2.2.2-28	4.2.3-02
3.1.2.2.2-29	4.2.3-02
3.1.2.2.2-30	4.2.3-02
3.1.2.2.2-31	4.2.3-02
3.1.2.2.2-32	4.2.3-02
3.1.2.2.2-33	4.2.3-02
3.1.2.2.2-33	2.1-11
3.1.2.2.2-34	2.1-14
3.1.2.2.2-34	4.2.3-02
3.1.2.2.2-34	2.1-11
3.1.2.2.3-01	DELETED
3.1.2.2.3-02	DELETED
3.1.2.2.3-03	DELETED
3.1.2.2.3-04	DELETED
3.1.2.2.3-05	DELETED
3.1.2.2.3-06	DELETED
3.1.2.2.3-07	2.1-08
3.1.2.2.3-08	2.1-08
3.1.2.2.3-09	2.1-08
3.1.2.2.3-10	2.1-08
3.1.2.2.3-11	2.1-08
3.1.2.2.3-12	2.1-08
3.1.2.2.3-13	DELETED
3.1.3-01	4.2.2-01
3.1.3-02	4.2.2-01
3.1.4-01	2.1-01
3.1.4-01	2.1-02
3.1.4-01	2.1-03
3.1.4-01	2.1-04
3.1.4-01	2.1-05
3.1.4-01	2.1-06
3.1.4-01	2.1-07
3.1.4-01	2.1-09
3.1.4-02	DELETED
3.1.5-01	4.2.4-01
3.1.5-01	4.2.4-02
3.1.5-02	4.2.4-01
3.1.5-03	DELETED
3.1.5-04	DELETED
3.1.5-05	2.2-03
3.1.5-06	DELETED
3.1.5-07	DELETED
3.1.5-08	4.2.4-01
3.1.5-09	DELETED
3.1.5-10	2.2-03

3.1.5-11	2.2-03
3.1.5-12	4.2.3-06
3.1.6-01	2.3-01
3.1.6-02	2.3-03
3.1.6-03	2.3-02
3.1.6-03	2.1-13
3.1.6-04	DELETED
3.1.6-05	2.3-01
3.1.6-06	2.3-01
3.1.6-07	2.3-03
3.1.6-08	2.3-05
3.1.6-09	2.3-04
3.1.6-09	4.2.3-07
3.2.1-01	DELETED
3.2.1-02	DELETED
3.2.1-03	DELETED
3.2.1-04	DELETED
3.2.1-05	2.1-09
3.2.4-01	4.2.1-01
3.2.5-01	9

Table 4.1-1 Traceability matrix User requirements vs Specification Id

4.2 TRACEABILITY FROM SPECIFICATION REQUIREMENTS TO URD

For the specifications defined in [AD4], the reference vs the user requirements is reported in the following table.

Specification Id	User Requirement ID
2.1-01	3.1.2.2.1-04
2.1-01	3.1.2.2.1-07
2.1-01	3.1.2.2.2-04
2.1-01	3.1.4-01
2.1-02	3.1.2.2.2-05
2.1-02	3.1.4-01
2.1-03	3.1.2.2.1-07
2.1-03	3.1.2.2.2-06
2.1-03	3.1.4-01
2.1-04	3.1.2.2.1-06
2.1-04	3.1.2.2.2-07
2.1-04	3.1.4-01
2.1-05	3.1.2-01
2.1-05	3.1.4-01
2.1-06	3.1.2.2.1-15
2.1-06	3.1.2.2.2-13
2.1-06	3.1.2.2.2-14
2.1-06	3.1.2.2.2-15
2.1-06	3.1.4-01
2.1-07	3.1.2.2.2-24
2.1-07	3.1.4-01
2.1-08	3.1.2.2.3-07
2.1-08	3.1.2.2.3-08
2.1-08	3.1.2.2.3-09
2.1-08	3.1.2.2.3-10
2.1-08	3.1.2.2.3-11
2.1-08	3.1.2.2.3-12
2.1-09	3.1.2.2.1-05
2.1-09	3.1.2.2.2-21
2.1-09	3.1.2.2.2-22
2.1-09	3.1.4-01
2.1-09	3.2.1-05
2.1-10	3.1.2.2.1-14.1
2.1-11	3.1.2.2.2-03
2.1-11	3.1.2.2.2-04
2.1-11	3.1.2.2.2-06
2.1-11	3.1.2.2.2-07
2.1-11	3.1.2.2.2-08
2.1-11	3.1.2.2.2-13

2.1-11	3.1.2.2.2-14
2.1-11	3.1.2.2.2-24
2.1-11	3.1.2.2.2-33
2.1-11	3.1.2.2.2-34
2.1-13	3.1.6-03
2.1-14	3.1.2.2.2-34
2.2-01	3.1.2.2.1-01
2.2-01	3.1.2.2.1-02
2.2-01	3.1.2.2.1-03
2.2-02	3.1.2.2.1-18
2.2-02	3.1.2.2.1-19
2.2-03	3.1.5-05
2.2-03	3.1.5-10
2.2-03	3.1.5-11
2.3-01	3.1.2.2.1-11
2.3-01	3.1.2.2.1-20
2.3-01	3.1.6-01
2.3-01	3.1.6-05
2.3-01	3.1.6-06
2.3-02	3.1.6-03
2.3-03	3.1.6-02
2.3-03	3.1.6-07
2.3-04	3.1.2.2.2-23
2.3-04	3.1.6-09
2.3-05	3.1.2.2.2-23
2.3-05	3.1.6-08
2.4.3.2	3.1.2.2.2-06
3.3.5	3.1.2.2.1-07
4.2.1-01	3.1.2.1-24
4.2.1-01	3.2.4-01
4.2.2-01	3.1.2-01
4.2.2-01	3.1.2.1-02
4.2.2-01	3.1.2.1-05
4.2.2-01	3.1.2.1-08
4.2.2-01	3.1.2.1-10
4.2.2-01	3.1.2.1-11
4.2.2-01	3.1.2.1-12
4.2.2-01	3.1.2.1-14
4.2.2-01	3.1.2.1-17
4.2.2-01	3.1.2.1-18
4.2.2-01	3.1.2.1-19
4.2.2-01	3.1.2.1-26
4.2.2-01	3.1.2.1-28
4.2.2-01	3.1.2.1-30
4.2.2-01	3.1.2.1-31

4.2.2-01	3.1.2.1-33
4.2.2-01	3.1.2.2.1-16
4.2.2-01	3.1.2.2.1-17
4.2.2-01	3.1.3-01
4.2.2-01	3.1.3-02
4.2.2-02	3.1.2.1-03
4.2.2-02	3.1.2.1-04
4.2.2-02	3.1.2.1-06
4.2.2-02	3.1.2.1-09
4.2.2-02	3.1.2.1-23
4.2.2-02	3.1.2.1-35
4.2.2-02	3.1.2.1-37
4.2.2-03	3.1.2.1-34
4.2.3-01	3.1.2.1-01
4.2.3-02	3.1.2-01
4.2.3-02	3.1.2.2.1-10
4.2.3-02	3.1.2.2.1-12
4.2.3-02	3.1.2.2.1-13
4.2.3-02	3.1.2.2.1-14.1
4.2.3-02	3.1.2.2.1-14.2
4.2.3-02	3.1.2.2.1-14.3
4.2.3-02	3.1.2.2.1-14.4
4.2.3-02	3.1.2.2.1-14.5
4.2.3-02	3.1.2.2.2-25
4.2.3-02	3.1.2.2.2-26
4.2.3-02	3.1.2.2.2-27
4.2.3-02	3.1.2.2.2-28
4.2.3-02	3.1.2.2.2-29
4.2.3-02	3.1.2.2.2-30
4.2.3-02	3.1.2.2.2-31
4.2.3-02	3.1.2.2.2-32
4.2.3-02	3.1.2.2.2-33
4.2.3-02	3.1.2.2.2-34
4.2.3-03	3.1.2.2.2-01
4.2.3-03	3.1.2.2.2-02
4.2.3-03	3.1.2.2.2-03
4.2.3-03	3.1.2.2.2-04
4.2.3-03	3.1.2.2.2-05
4.2.3-03	3.1.2.2.2-06
4.2.3-03	3.1.2.2.2-07
4.2.3-03	3.1.2.2.2-08
4.2.3-03	3.1.2.2.2-09
4.2.3-03	3.1.2.2.2-13
4.2.3-03	3.1.2.2.2-14
4.2.3-03	3.1.2.2.2-15

4.2.3-03	3.1.2.2.2-21
4.2.3-03	3.1.2.2.2-22
4.2.3-03	3.1.2.2.2-24
4.2.3-04	3.1.2-02
4.2.3-05	3.1.2-04
4.2.3-06	3.1.2.1-36
4.2.3-06	3.1.2.1-38
4.2.3-06	3.1.5-12
4.2.3-07	3.1.2.2.2-23
4.2.3-07	3.1.6-09
4.2.4-01	3.1.2-05
4.2.4-01	3.1.5-01
4.2.4-01	3.1.5-02
4.2.4-01	3.1.5-08
4.2.4-02	3.1.5-01
4.2.4-03	3.1.2.1-20
4.4.2-01	3.1.1-05
9	3.2.5-01
DELETED	3.1.1-01
DELETED	3.1.1-02
DELETED	3.1.1-03
DELETED	3.1.1-04
DELETED	3.1.2-03
DELETED	3.1.2.1-07
DELETED	3.1.2.1-13
DELETED	3.1.2.1-15
DELETED	3.1.2.1-16
DELETED	3.1.2.1-21
DELETED	3.1.2.1-22
DELETED	3.1.2.1-25
DELETED	3.1.2.1-27
DELETED	3.1.2.1-29
DELETED	3.1.2.1-32
DELETED	3.1.2.2.1-08
DELETED	3.1.2.2.1-09
DELETED	3.1.2.2.2-10
DELETED	3.1.2.2.2-11
DELETED	3.1.2.2.2-12
DELETED	3.1.2.2.2-16
DELETED	3.1.2.2.2-17
DELETED	3.1.2.2.2-18
DELETED	3.1.2.2.2-19
DELETED	3.1.2.2.2-20
DELETED	3.1.2.2.3-01
DELETED	3.1.2.2.3-02

DELETED	3.1.2.2.3-03
DELETED	3.1.2.2.3-04
DELETED	3.1.2.2.3-05
DELETED	3.1.2.2.3-06
DELETED	3.1.2.2.3-13
DELETED	3.1.4-02
DELETED	3.1.5-03
DELETED	3.1.5-04
DELETED	3.1.5-06
DELETED	3.1.5-07
DELETED	3.1.5-09
DELETED	3.1.6-04
DELETED	3.2.1-01
DELETED	3.2.1-02
DELETED	3.2.1-03
DELETED	3.2.1-04

Table 4.2-1 Traceability matrix Specification Id vs User requirements

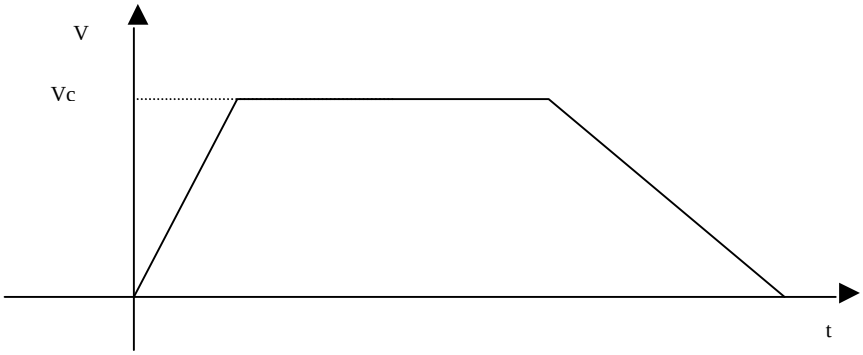
ANNEX A POSITION CONTROL

When the carousel rotation or drill translation is commanded to perform a positioning, SD2_FSW shall generate position sequence at C_MRFR Hz (as per Tab. B-1) based on a desired max. speed and proper ramping up/down. During motion the relevant resolver is read with a frequency of C_MRFR Hz.

Hereunder, Vc is the coasting speed specified in the drill/ carousel motion command.

Carousel Position Control

For the carousel position control, the following speed profile shall be applied:



The carousel speed profile consists of three phases: an acceleration phase, a coasting speed phase and a deceleration phase.

1) During the acceleration phase, an increasing ramp starting from speed zero to speed Vc shall be generated, step by step by means of successive speed commands at the rate of C_MRFR Hz (as per Tab. B-1)
2) At coasting speed phase, the Vc speed shall be used as speed command
3) during the deceleration phase, it shall be applied the following speed:

V = Max(C_CAR_LOWER_SPEED,
Vc*|Carousel_Current_Pose –Carousel_Target_Pose|/C_CAR_RAMP_DOWN_TH)

(see Table B-1 for the constant definition)

4) the decreasing ramp shall start when

|Carousel_Current_Pose –Carousel_Target_Pose| <= C_CAR_RAMP_DOWN_TH

This check shall be evaluated both during the acceleration phase and during the coasting speed phase.

5) the motion ends when

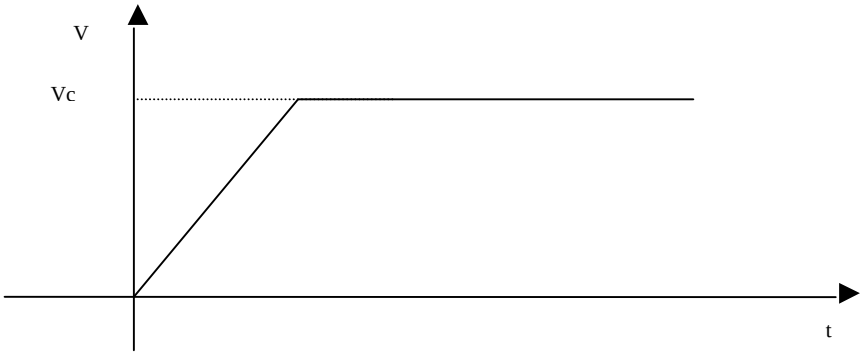
|Carousel_Current_Pose – Carousel_Target_Pose| <= C_CAR_TARGET_TH

so that the maximum positioning error is C_CAR_TARGET_TH

6) it shall be checked that the deceleration ramp takes less than C_CAR_RAMP_DOWN_MAX_DURATION

Drill translation Position Control

For the drill translation position control, the following speed profile shall be applied:



The drill translation speed profile consists of two phases: an acceleration phase and a coasting speed phase.

1) During the acceleration phase, an increasing ramp starting from speed zero to speed Vc shall be generated, step by step by means of successive speed commands at the rate of C_MRFR Hz (as per Tab. B-1)
2) At coasting speed phase, the Vc speed shall be used as speed command
3) the motion ends when

   Drill_Current_Pose >= Drill_Target_Pose

Note that the maximum positioning error for drill translation is the length covered in 1/C_MRFR, so at the maximum speed 1209 RPM in 250 ms the error is 8.6 [1/100 mm]

ANNEX B VALUES & PARAMETERS

For general referring, in the following tables, SD2 parameters are reported. The values of them will be included in SD2- User Manual

Name	***Meaning***
C_ZECTO	zero position carousel rotation tolerance
C_DOVTO	drill axis to oven axis position tolerance
C_DDUTO	drill axis to dummy oven axis position tolerance
C_ZEDTO	zero position drill translation tolerance
C_MRFR	Motion regulation frequency
C_CDMS_TIMEOUT	Timeout for CDMS successfull communication
C_CDMS_NUM_RETRY	maximum number of retries to be used in the CDMS communication protocol
C_COMMAND_PERIOD	period of specific command processor
C_LOAD_MAX_NUM	number maximum of mission plan re-load
C_HITB_DEF_ACQ	Default HITB acquisition period
C_SC_DATE_NUM_FRAMES	maximum number of scientific data frames contained into HITB buffer
C_ZERO_DT_SPEED	Speed of drill translation for executing the ZERO command
C_ZERO_DT_TORQUE	Torque of drill translation for executing the ZERO command
C_ZERO_CAR_SPEED	Speed of carousel for executing the ZERO command
C_ZERO_CAR_TORQUE	Torque of drill translation for executing the ZERO command
C_MAX_CDMS_MESSAGE	Dimension of specific command queue
C_MAX_MP_WORDS	Maximum dimension of stored telecommand sequence
C_RESOLVER_POWER_DELAY	Time required for resolver power on
C_VOLCHK_SWITCH_PERIOD	acquisition period of upper volume checker micro-switch

C_VCAC_TORQUE	torque to be used in VCAC command for volume checker up motion
C_VCAC_SPEED	speed to be used in VCAC command for volume checker up motion
C_SRDT	Drill translation ampling range, as specified in UR-3.1.2.2.1-1
C_DRTD	Drill translation discharge range, as specified in UR-3.1.2.2.1-1
C_ARDT	Drill translation re-arm range, as specified in UR-3.1.2.2.1-1
C_DFDT	Drill translation default range, as specified in UR-3.1.2.2.1-1
C_LANDG_MIN, C_LANDG_MAX	Range causing interference with landing gear legs
C_CAR_RAMP_DOWN_TH	Threshold used for carousel position control. When |Car_Cur_Pos–Car_Target_Pos| <= C_CAR_RAMP_DOWN_TH, then the carousel decelerating phase starts
C_CAR_LOWER_SPEED	Carousel lower speed level to be used during the carousel deceleration phase
C_CAR_TARGET_TH	Threshold used for checking the carousel end of motion
C_CHK_DR_MIN_SPEED	Minimum drill rotation speed used for drill rotation measurement
C_CHK_DR_PERIOD	Execution period of drill rotation check
C_CHK_DR_SPEED_TOL	Tolerance used for drill rotation speed check
C_NUM_PULSE_PER_ROUND	number of pulses for round of drill rotation
C_CHK_DT_MIN_SPEED	Minimum drill translation speed used for drill translation speed check
C_CHK_DT_PERIOD	Execution period of drill translation check
C_CHK_DT_SPEED_TOL	Tolerance used for drill translation speed check
C_CHK_CAR_MIN_SPEED	Minimum carousel speed used for carousel speed check
C_CHK_CAR_PERIOD	Execution period of carousel check
C_CHK_CAR_SPEED_TOL	Tolerance used for carousel speed check

C_CAR_RAMP_DOWN_MAX_DURATION	Max duration of carousel ramp down phase
C_DT_RECOVERY_TORQUE	Torque to be used when drill translation speed check fails first time
C_SECTION_SWITCH_DELAY	delay between switching of two electronics section
C_SET_SPEED_DELAY	delay after set-speed settings
C_POWER_SWITCH_DELAY	delay after power section switching
C_X0	drill position used in the UR-3.1.2.2.2-1

Table B-1 Parameters table