LUMIR
Harmony in Differences

ETRI

Korea Lunar Exploration Program

DTN

SBC Failure Mode, Effects, and Criticality Analysis

Date: 15 Oct. 2018

Doc. No: KPLO-D1-554-029
Issue: 1.0
Total page: 14

Superseding Revised

Prepared By:

June-Tae Park Date
DTN Payload Engineer, Lumir

Reviewed By:

Chang-Soo Lee Date
DTN Product Assurance, Lumir

Dae-Soo Oh Date
DTN Project Manager, Lumir

Approval Signature:

Cheol-Oh Jeong Date
DTN Product Assurance, ETRI

Jin-Ho Jo Date
DTN Project Leader, ETRI

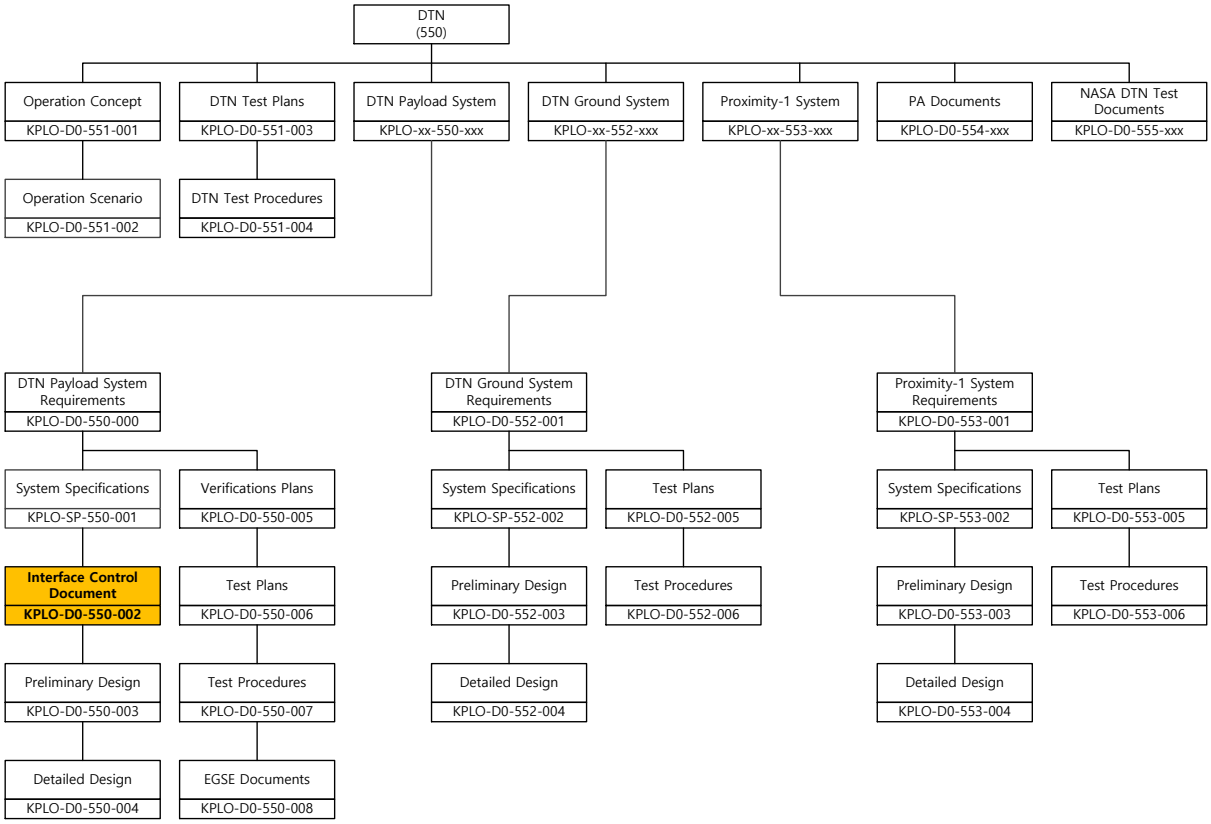
Original CDMO Release_____

Revision History

Version	Author(s)	Date	Description
D-00	Dae-Soo Oh	2016. 10. 07	Draft
P-00	Dae-Soo Oh	2016. 11. 23	FMECA Table add
P-01	Jae-Won Jang	2017. 09. 06	FMECA Table TM/TC Interface add
P-02	Jae-Won Jang	2018. 01. 16	FMECA Table Power short mode add
1.0	Jun-Tae Park	2018. 10. 15	FMECA Table Bus Interface add

Revision/Change Records			
Version	Date	Revision/Change Description	Pages
D-00	2016. 10. 07	Draft	All
P-00	2016. 11. 23	FMECA Table add	13, 14
P-01	2017. 09. 06	FMECA Table TM/TC Interface add	13, 14
P-02	2018. 01. 16	FMECA Table Power short mode add	13, 14
1.0	2018. 10. 15	FMECA Table Bus Interface add	13, 14

Documents Tree



Contents

Figures

Tables

1 INTRODUCTION

1.1 SCOPE

This document summarizes FMECA for the Single Board Computer (SBC) to be developed for the DTN. FMECA analysis procedures and documentation shall be performed in accordance with ECSS-Q-30-02 and MIL-STD-1629.

1.2 DTN Overview

The mission of DTN is to validate DTN communication protocols by space-link testing through KPLO. So DTN operations are focused on testing the DTN protocols using KPLO space-links.

2 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

	Document No.	Title
AD-1	KPLO-D0-210-003	User Requirements Document (KARI)
AD-2	KPLO-D0-524-008	User Requirements Document (ETRI)

2.2 REFERENCE DOCUMENTS

	Document No.	Title
RD-1	MIL-STD-461E	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
RD-2	MIL-STD-462D	Measurements of Electromagnetic Interference Characteristics
RD-3	ECSS-E-ST-10-06C	Space engineering Technical Requirements specification
RD-4	ECSS-Q-60-11A	Derating and End of Life parameter drifts-EEE Components
RD-5	MIL-HDBK-217	Reliability Prediction for Electronic Equipment
RD-6	ECSS-Q-ST-30-02	Failure Modes, Effects and Criticality Analysis (ESA Document)
RD-7	MIL-STD-1629	Failure Modes, Effects and Criticality Analysis(US Military Document)

3 ACRONYMS AND ABBREVIATIONS

AMS	Asynchronous Message Service
AOS	Advanced Orbiting System
BP	Bundle Protocol
BSS	Bundle Streaming Service
CCSDS	Consultative Committee for Space Data Systems
CFDP	CCSDS File Delivery Protocol
DCC	DTN Control Center
DTN	Delay(Disruption) Tolerant Network
DTNPL	DTN Payload
IP	Internet Protocol
KPLO	Korea Pathfinder Lunar Orbiter
LCM	Lander Communication Model
LTP	Liklider Transmission Protocol
M&C	Monitor & Control
RCM	Rover Communication Model
SLE	Space Link Extension
TBC	To Be Confirmed
TBD	To Be Defined
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4 FMECA Analysis

The Configuration of SBC (Single Board Computer) is shown as below (Figure 4-1)

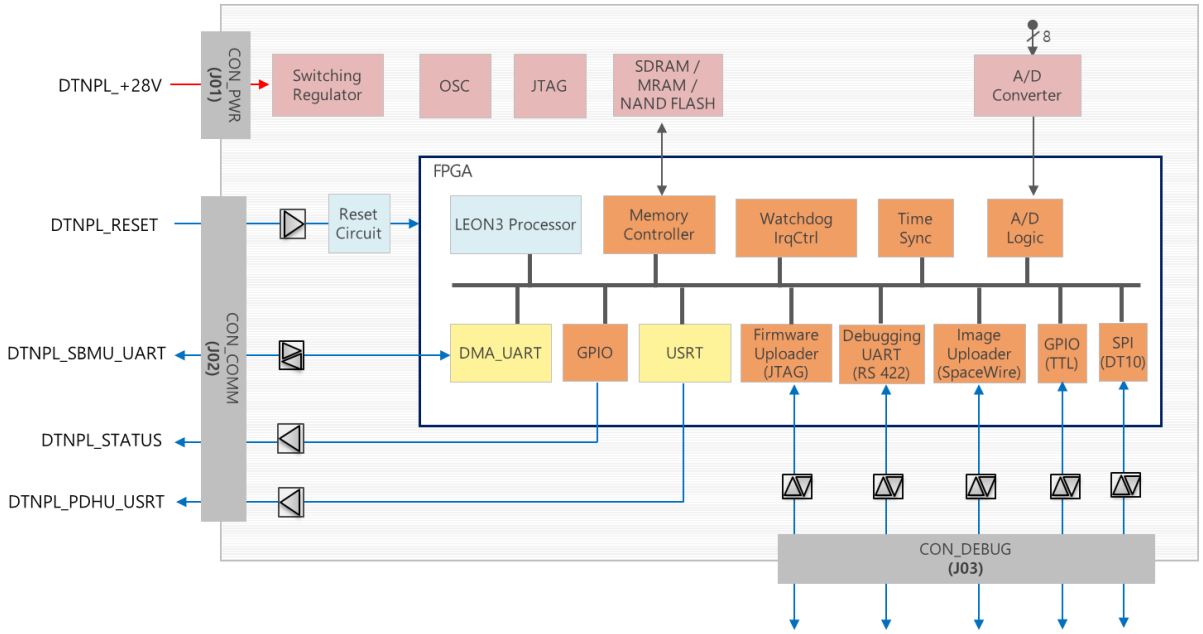


Figure 4-1 SBC Configuration

4.1 Qualitative Approach

Failure modes identified in the FMEA are assessed in terms of probability of occurrence when specific parts configuration or failure rate data are not available.

Individual failure mode probabilities of occurrence should be grouped into distinct, logically defined levels, which establish the qualitative failure probability level for entry into the appropriate CA worksheet column.

Probability of occurrence levels are defined as follows

(i) Level A - Frequent. A high probability of occurrence during the item operating time interval. High probability may be defined as a single failure mode probability greater than 0.20 of the overall probability of failure during the item operating time interval.

(ii) Level B - Reasonably probable. A moderate probability of occurrence during the item operating time interval. Probable may be defined as a single failure mode probability of occurrence which is more than 0.10 but less than 0.20 of the overall probability of failure during the item operating time.

(iii) Level C - Occasional. An occasional probability of occurrence during item operating time interval. Occasional probability may be defined as a single failure mode probability of occurrence which is more than 0.01 but less than 0.10 of the overall probability of failure during the item operating time.

(iv) Level D - Remote. An unlikely probability of occurrence during item operating time interval. Remote probability may be defined as a single failure mode probability of occurrence which is

more than 0.001 but less than 0.01 of the overall probability of failure during the item operating time.

(v) Level E - Extremely unlikely. A failure whose probability of occurrence is essentially zero during item operating time interval. Extremely unlikely may be defined as a single failure mode probability of occurrence which is less than 0.001 of the overall probability of failure during the item operating time.

4.2 Severity Categories

A severity category(Table 4-1) shall be assigned to each failure mode and item according to the failure effect. The effect on the functional condition of the item under analysis caused by the loss or degradation of output shall be identified so the failure mode effects will be properly categorized. For lower levels of indenture where effects on higher indenture levels are unknown, a failure's effect on the indenture level under analysis shall be described by the severity classification categories.

Table 4-1 DTN Severity Category

Severity	Category	Definition
Catastrophic	1	Failure modes that could result in serious injury or loss of life or loss of launch vehicle.
	1R	Failure modes of identical or equivalent redundant hardware item that, if all failed, could result in Category 1 effects.
	1S	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and leads to Severity Category 1 consequences.
Critical	2	Failure modes that could result in loss of one or more mission objectives.
	2R	Failure modes of redundant hardware items that could result in Category 2 effects if all failed.
Significant	3	Failure modes that could cause degradation to mission objectives.
Minor	4	Failure modes that could result in insignificant effect to mission objectives.
Negligible	5	No effect

Suffix 'R' means failure mode related to redundant function and Suffix 'S' means failure mode related to safety monitoring function.

4.3 Failure Mode Criticality Number

The fraction of the part failure rate related to the particular failure mode under consideration shall be evaluated by the analyst and recorded. The failure mode ratio is the probability expressed as a decimal fraction that the part or item will fail in the identified mode. If all potential failure modes of a particular part or item are listed, the sum of the values for that part or item will equal one.

Individual failure mode multipliers may be derived from failure rate source data or from test and operational data. If failure mode data are not available, the values shall represent the analyst's judgment based upon an analysis of the item's functions.

4.4 SBC FMECA Table

I.D. Number	Item	Module / Function	Failure Modes	Operation Phase	Failure Effects		Failure Detection Methods	Compensating Provision	Severity	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ, FIT)	Occurrence	Operation Time (Hours)	Criticality Number
					Local Effects (SBC)	End Effects (BUS)									
101		Main Controller	RTG4 FPGA Gate failure (Gate Single Event Error)	D, E	No Effect	No Effect	Automatically Detection TMR circuit in RTG4 FPGA	Automatically Correction by TMR circuit in RTG4 FPGA	5	0.00	0.02	4.09	0.1	8760.00	0.00E+00
102		Application Software Storage	SDRAM failure (Memory Single bit Error at one time)	D, E	No Effect	No Effect	Detection by EDAC Algorithm implemented in FPGA	Correction by EDAC Algorithm implemented in FPGA	5	0.00	0.03	5.72	0.2	8760.00	0.00E+00
103			SDRAM failure (more than Memory Double bit Error at one time)	D, E	Automatically H/W Reset (SBC Re-start)	No Effect	Detection by EDAC Algorithm implemented in FPGA	Automatically H/W Reset signal generation by EDAC Algorithm implemented in FPGA	3	0.10	0.03	5.72	0.2	8760.00	1.33E-07
104	SBC	Boot Software	MRAM failure (Memory Single bit Error at one time)	D, E	No Effect	No Effect	Detection by EDAC Algorithm implemented in FPGA	Correction by EDAC Algorithm implemented in FPGA	5	0.00	0.03	5.72	0.2	8760.00	0.00E+00
105			MRAM failure (more than Memory Double bit Error at one time)	D, E	SBC Malfunction (SBC Fail)	No Effect	KPLO Detection by no LifeSign	SBC reboot	2	1.00	0.03	5.72	0.2	8760.00	1.33E-06
106			MRAM failure (Sing Event Latch up)	D, E	SBC Malfunction (SBC Fail)	No Effect	KPLO Detection by no LifeSign	MRAM Latch-up Current Limiter	2	1.00	0.03	5.72	0.2	8760.00	1.33E-06
107		Mission Data Storage	NAND Flash failure (Single bit Error at one time)	D, E	No Effect	No Effect	Detection by EDAC Algorithm implemented in FPGA	Correction by EDAC Algorithm implemented in FPGA	5	0.00	0.03	5.72	0.2	8760.00	0.00E+00
108			NAND Flash failure (more than Memory Double bit Error at one time)	D, E	Mission Data Loss	No Effect	Detection by EDAC Algorithm implemented in FPGA	Discard crashed mission data and using another mission data	4	0.05	0.03	5.72	0.2	8760.00	6.63E-08

I.D. Number	Item	Module / Function	Failure Modes	Operation Phase	Failure Effects		Failure Detection Methods	Compensating Provision	Severity	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ, FIT)	Occurrence	Operation Time (Hours)	Criticality Number
					Local Effects (SBC)	End Effects (BUS)									
109		Operation Freq. Generation	OSC failure	D, E	SBC Malfunction (SBC Fail)	No Effect	KPLO Detection by no LifeSign	SBC reboot	2	1.00	0.07	15.98	1.2	8760.00	1.04E-05
110		TM/TC Interface	RS422 Driver Failure	D, E	TMTC Data Loss	No Effect	KPLO Detection by no TMTC Response	Fail Safe Circuit implemented	5	0.00	0.08	17.81	1.5	8760.00	0.00E+00
111			RS422 Receiver failure	D, E	TMTC Data Loss	No Effect	KPLO Detection by no TMTC Response	Fail Safe Circuit implemented	5	0.00	0.08	16.82	1.3	8760.00	0.00E+00
112			Haness Short or Open		TMTC Data Loss (Mission Data Loss)	No Effect	KPLO Detection by no TMTC Response	Tightly Connector Locking Mechanism applied using Space grade DSUB	4	0.05	0.08	17.82	1.5	8760.00	6.45E-07
113		PDHU Interface	RS422 Driver Failure	D, E	Mission Data Loss	No Effect	KPLO Detection by no TMTC Response	Fail Safe Circuit implemented	5	0.00	0.08	17.81	1.5	8760.00	0.00E+00
114			RS422 Receiver failure	D, E	Mission Data Loss	No Effect	KPLO Detection by no TMTC Response	Fail Safe Circuit implemented	5	0.00	0.08	16.82	1.3	8760.00	0.00E+00
115	SBC		Haness Short or Open		Mission Data Loss	No Effect	KPLO Detection by no TMTC Response	Redundancy RS422 Ch	4	0.05	0.08	17.82	1.5	8760.00	6.45E-07
116		Analog	Analog Mux	D, E	Not gathering Analog information such as temperature, etc Information loss	No Effect	Detection by SBC S/W	No using Analog Information	4	0.05	0.08	17.81	1.5	8760.00	6.44E-07
117			ADC	D, E	Not gathering Analog information such as temperature, etc Information loss	No Effect	Detection by SBC S/W	No using Analog Information	4	0.05	0.08	17.81	1.5	8760.00	6.44E-07
118		Power Interface	Power line Short or Open	D, E	SBC Malfunction (SBC Fail)	No Effect	KPLO Detection by no LifeSign	When the output is overloaded or shorted the current limit is activated.	2	1.00	0.07	15.07	1.1	8760.00	9.22E-06
119			Harness Short or Open	D, E	SBC Malfunction (SBC Fail)	No Effect	KPLO Detection by no LifeSign	Over current protection circuit implemented	3	0.10	0.07	16.07	1.2	8760.00	1.05E-06
120		TM/TC Interface (Bi-level)	Transitor Failure	D, E	Bi-level TM (SBC Status) Loss	No Effect	KPLO Detection by no Heartbeat Response	No Detection of SBC Status	4	0.05	0.08	17.81	1.5	8760.00	6.44E-07
121			Transitor Failure	D, E	Bi-level TC (SBC Reset) Loss	No Effect	KPLO Detection by Reset Count Response	No control of SBC reset	4	0.05	0.08	17.81	1.5	8760.00	6.44E-07