



Detecting Failure Modes, Effects and Criticality Analysis of LEO Spacecraft Solar Array System

Ahmed Mokhtar Mohamed^{*}, Fawzy ElTohamy H. Amer[†], R. M. Mostafa[‡]

Abstract: In this paper the reliability issue of a solar array of LEO spacecraft was analyzed with Failure Modes Effects and Criticality Analysis (FMECA) to ensure that the solar array will deliver the required power to the spacecraft until the end of life without failures. The main failure modes, their effects and criticalities were illustrated. A fault tree was built. Both qualitative and the quantitative analysis of the fault tree were performed. The probability of the top event, the structural importance and the critical importance coefficients of different basic events were detected and overcome by protective actions. According to the analyses, the main reasons of the satellite solar array failure and the list of the critical components were presented. The effects of different failures were classified according to the severity and the criticality of the faults. Recommendations for improving solar arrays' reliability were provided for reliability design and structure improvement of the satellite solar array.

Keywords: Failure Modes Effects and Criticality Analysis (FMECA), Solar array system, LEO spacecraft

1. Introduction

Within the subject of risk analysis, we search for treatment of the process of finding, organizing, and categorizing the set of risk scenarios. It should include within itself the well-known standard methods of scenario identification such as fault trees, FMEA, and failure mode, effects, and criticality analysis (FMECA) [1].

Failure mode and effects analysis (FMEA) and failure mode, effects, and criticality analysis (FMECA) are reliability-based methods that are widely used for reliability analysis of systems, subsystems, and individual components of systems. They constitute an enabling mechanism with which to identify the multiple paths of system failures [1].

Indeed, a requisite for an effective risk assessment process is to identify all conceivable failure modes of a system (through all of its subsystems and components as well as the interaction with its environment), in this regard, hierarchical holographic modeling (HHM) constitutes a critical building block in a modified FMECA [2].

An effective HHM should be performed by a team of cross disciplinary experts. Such a team is needed for the initial steps of FMECA, although the quantitative components of the FMECA are more simplistic than the quantitative risk analysis methods [1].

^{*} Egyptian Armed Forces, Egypt, mostafamokhtar100@gmail.com

[†] Egyptian Armed Forces, Egypt, ftohamy72@yahoo.com

[‡] Professor of Electrical Engineering. Faculty of Industrial Education, Beni-Suef University, Egypt, R_mostafa05@yahoo.com

The qualitative parts of FMECA are quite effective and powerful. They force engineers and other quality control professionals to follow a methodical systemic process with which to track, collect, and analyze critical information that ultimately leads to effectively assessing and managing risks of failure modes of large and small systems [3].

The fact that the military (until 1998) as well as professional associations have embraced FMECA and developed standards to guide the users of these methods attests to their value [1].

The MIL-STD-1629A [1980] was the standard for the US military from November 1980 to 1998 (superseding MIL-STD- 1629 (SHIPS) dated 1 November 1974, and MIL-STD-2070 (AS) dated 12 June 1977) [3].

An FMECA can be described as a systematic group of activities intended to:

- 1- Recognize and evaluate the potential failure(s) of an item or process and the effects of that failure.
- 2- Identify actions that could eliminate or reduce the likelihood of the potential failure occurring (probability of occurrence)
- 3- It defines who, what, why, when, and how related to the performance of a Failure Modes and Effects Analysis (FMECA) and establishing a Critical Items List (CIL).

Why an FMECA is performed – the underlying intent of performing an FMECA When an FMECA performed – When in the Program Cycle FMECAs are performed.

FMECAs are performed during the preliminary and detailed design phases of a program have as a purpose the iteration of the design to remove critical and high priority failure modes, FMECA iterations performed later are used to validate the design has no critical or high priority failure modes remaining after corrective action has been implemented [1,3].

Who performs the FMECA – which personnel are involved in performing each type of FMECA What is contained in an FMECA , the expected information that is input and output during the performance of an FMECA How the FMECA is performed , the actual step by step approach to performing an FMECA The Critical Items List collects information developed by the FMECA identifying specific systems, sub-systems, functions, components, piece parts, and/or processes that if failed present risk to human life , mission success, or destruction of spacecraft.

THE main goal from FMECA is used for identifying, eliminating, or mitigating unacceptable failure modes (those leading to failure of the mission), FMECA provides a framework to review the design, identify potential failure modes, and assess the effects of the failures [3].

A system-level assessment is performed to determine if the system is robust to the identified failure modes or requires remediation, this work is performed iteratively over the program life cycle in a collaborative effort between the acquisition team (customer), contractor's system/subsystem engineering, unit engineering and reliability engineering, teams in an effort to ensure the system design is robust, will meet customer requirements, and conforms to program-level cost and schedule milestones as shown in Figure (1) [4].

The purpose of FMECAs is to determine, characterize, and document possible failure modes their effects on mission success through a systematic analysis of the design during initial trades, preliminary design, detailed design, and changes to design after CDR [3,4].

The analysis is intended to identify design changes necessary to meet reliability requirements in a timely manner and to foster interchange of failure mode information with program activities such as design, system engineering, system safety, integration & test, reliability block diagram development, failure reporting, and corrective action (FRACAS) and fault management [4].

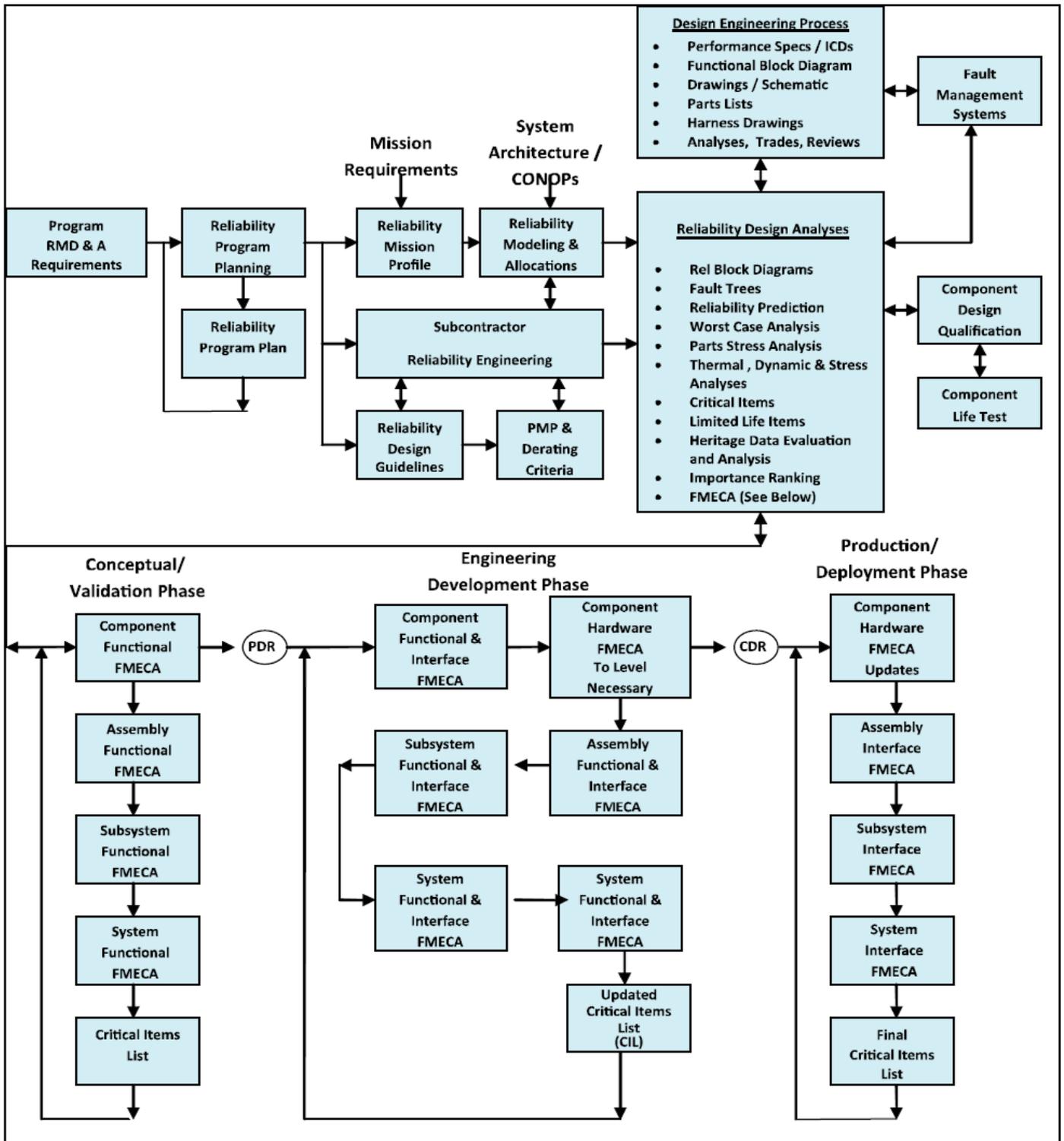


Figure 1. Reliability engineering/FMECA process flow [4]

Severity Category

$$\text{FMEA} + \text{C} = \text{FMECA}$$

C = Criticality = Risk = Severity Level/Probability of Occurrence criticality is typically qualitative and indicated by the severity level, it can also be quantitative and indicated by the probability of occurrence, examples are shown in Table 1 and Table 2 [5,6].

Table [1]: Severity Category [7,8]

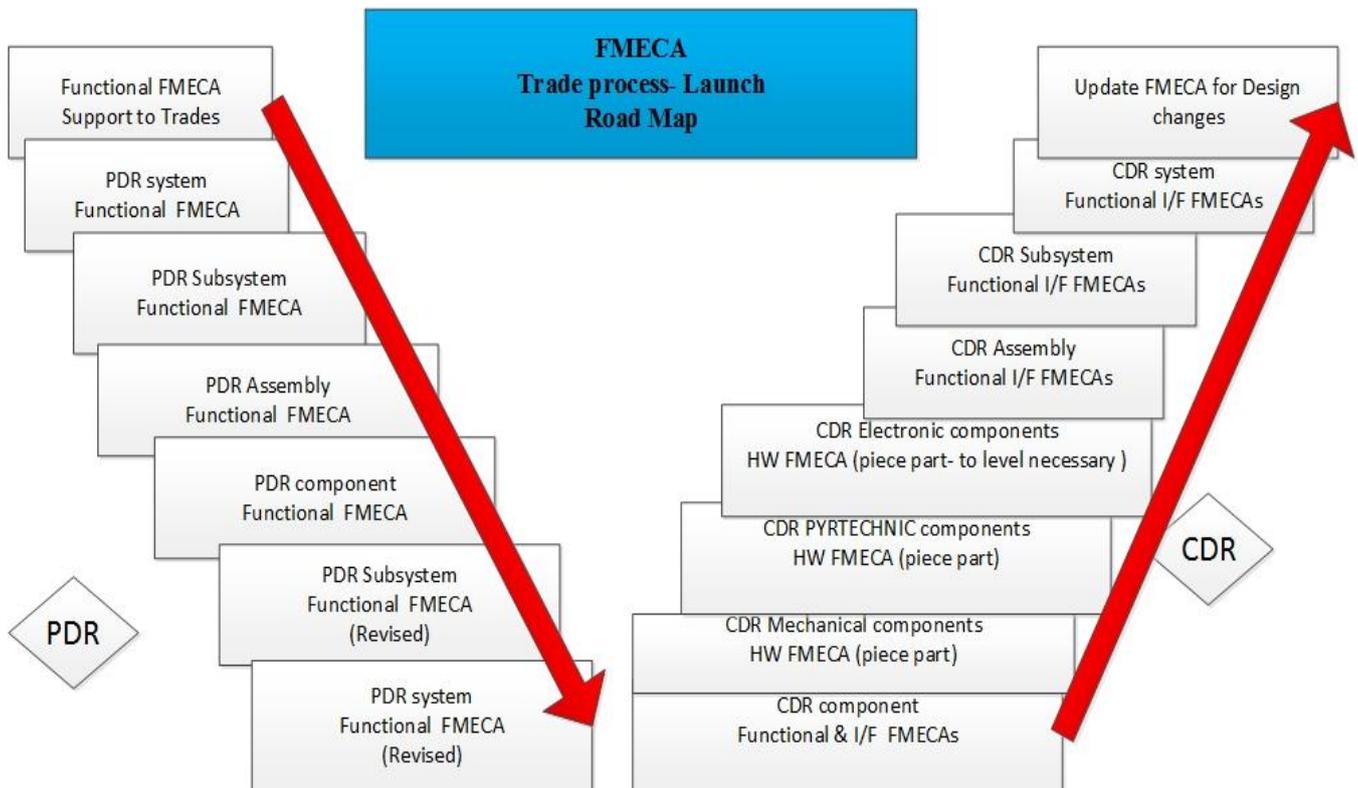
Severity Category	Severity Level
Catastrophic Loss of Mission or Life	1
Degraded Mission	2
Loss of Redundancy	3
Negligible	4

Table [2]: Probability Category [7,8]

Level	Probability of Occurrence
Probable	$P_0 > 0.01$
Occasional	$0.0001 \leq P_0 \leq 0.01$
Remote	$0.00001 \leq P_0 \leq 0.0001$
Extremely Remote	$P_0 \leq 0.00001$

On space vehicles, FMECAs are used to help identify and limit critical failures/single point failures, prevent failure mode propagation and identify reliability critical items, for single-point failures that cannot be designed out or mitigated, critical-item control plans (CICP) are developed and executed to minimize failure mode probability [9], (Figure 2).

The objective of a FMECA is to identify the way failures could occur (failure modes) and the consequences of the failures modes on space vehicle performance (failure effect) and the severity effect on mission objectives (criticality), it is usually based on the case upon which failure effects at the system level are caused by failure modes at lower levels, criticality is typically a qualitative measure (severity) and is normally accompanied by the failure mode's probability of occurrence for severity levels 1 and 2.



1- Assembly Level Means deployed solar arrays , Antenna

2- "To Level Necessary" for internal redundancy components and any components with HW failure detection & recovery isolation circuit

Figure 2. FMECA Trade process to launch road map

2. Solar Array Failure Modes, Effects and Criticality Analysis

Detail structure analysis

The SA design case consists of following details, influencing on its reliability:

- 1- The photovoltaic array (current-forming part of the SA), developed according to Design of photovoltaic of the SC.
- 2- SC body (frame structure), on which PVA is placed. It includes honeycomb panel attached to SC by hinges with springs for deployment, SA deployment mechanisms and 2 metallization buses of SA panel connected to the SC metallization terminal.

The following elements were revealed in FMECA; their failures can have an influence on the solar array operability:

So, it should be checked to remove the criticality or ensure the criticality

- 1- solar cells
- 2- Bus bar between solar cells
- 3- points of welding
- 4- points of soldering

- 5- integral bypass diode
- 6- blocking device
- 7- wires

The detail failure is considered as failure to comply with the purpose requirements, the SA constituent element failure is considered as failure to comply with the functions, mentioned in regulations and/or required for the major task fulfillment [9].

FMECA was conducted according to regulations with SA constituent element qualitative analysis and forming the list of critical elements, the decision about the element inclusion in the list of critical elements was accepted on the ground of many years' SA development experience in the following cases:

- 1- The element single failure leads to SA failure.
- 2- The element reliability requires the periodic confirmation of manufacturing process stability.
- 3- The element reliability requires the experimental confirmation.
- 4- The low level of the element reliability, which leads to detail durability reduction.

Note: - not one wire connects each elementary generator to the bus.

3. Solar Cells Failures

Solar cells failures analysis is presented in the Table (3).

The failure of the solar cells in the string itself can't cause the failure of the whole string but may cause durability reduction. Its effect reveals only with the integral bypass diode which is found in each cell so the failure of one or more cell will lead just to reduce the voltage of the string but not the complete failure of this string or the SA. Therefore, such mode failure is not critical.

SC of solar cell cause only the reduction of the voltage of the string, what allows to consider this failure mode as well to be partly removed and non-critical. At worst-case, it is considered, causes the string failure, the made analysis allows not including the solar cell failure into the list of the critical elements [10].

This method continues until the improvement method has converged and an optimum system is found.

4. The Integral Bypass Diode Failures

The bypassing discharge chain includes 2 discharge BD and fusing element link. With the beginning of SC at the diode, the fusing link should response with the bypassing chain disconnection.

BD discharge chain failures analysis is presented in Table 4.

The bypass diode at the solar cell, which is possible in the case of even disconnection, causes the string failure as it will be open circuit in the string and this in case of the cell failure but in case of the probably work of the cell the open circuit of the integral diode will not appear, but in case of the short circuit of the integral diode we will lose just one cell element and this in case of the cell working probably or not and this failure will lead to reduce the total voltage of the string and also the current delivered by the string The at worst causes the single string failure [10].

The made analysis of all modes of integral bypass diode failure allows not to include it into the list of the critical elements.

Table [3]: Solar cells failures

Failure characteristics	Failure modes	
	Disconnection fault	Short circuit
Causes	Manufacturing defect	Manufacturing defect
Features	Reduction of the voltage of the string	Reduction of the voltage of the string
Effect	In the case of the single failure – no effects In the case of the synchronous failure of the appropriate solar cells– string failure	String voltage reduction (at worst considered as string failure)
Effect elimination	In the case of synchronous failure of the appropriate cells the effects are no recoverable	The cells protection with the bypassing diode
Criticality	The single failure is allowed. In the case of synchronous failure of the appropriate cells one string failure is allowed. Uncritical	The single failure is allowed. Uncritical

Table [4]: The bypassing discharge chain

Failure characteristics	Failure modes	
	Disconnection fault	Short circuit
Causes	Manufacturing defect	Manufacturing defect
Features	Disconnection in the string, in case of the solar cell failure, but in case of normal operation it will not affect or appear	Losing of the voltage of this cell and reduce of the total voltage of the string voltage
Effect	In the case of the single failure there will be disconnection on the string in case of the solar cell failure, but in case of normal operation it will not affect or appear	Losing the voltage of this cell only
Effect elimination	Non- recoverable	Non- recoverable
Criticality	Failure is allowed. Uncritical	Failure is allowed. Uncritical

5. Blocking Device Failure Analysis

In case of failure of this blocking diode there will be two types of failure: -

- 1- short circuit: - this failure will not appear in case of the normal operation without failure of surrounding strings
- 2- open circuit: - this failure will lead to losses the whole string but it is possible as it permissible for one string failure, so by this analysis the blocking diode will not considered as critical element [11].

Table 5 presents the blocking device failure analysis.

Table [5]: Blocking device failure

Failure characteristics	Failure modes	
	Disconnection fault	Short circuit
Causes	Manufacturing defect	Manufacturing defect
Features	Reduction of the total delivered current by the corresponding generator	this failure will not appear in case of the normal operation without failure of any cell of this string
Effect	Reduction of the total delivered current by the corresponding generator, loose of one string element	Reduce the performance of the string due to the reverse current from the surrounding string in case of 1 solar cell failure in the string because the string will be considered as a load for the other strings as its voltage will be reduced and in the end losing of this string and this is permissible
Effect elimination	Non -recoverable	Non- recoverable
Criticality	The single failure is allowed. In the case of synchronous failure of the appropriate strings (excepting SC) such failure isn't allowed. Uncritical	The single failure is allowed. Uncritical
Criticality	The single failure is allowed. In the case of synchronous failure of the appropriate strings (excepting SC) such failure isn't allowed. Uncritical	The single failure is allowed. Uncritical

6. Bus Bar Between Solar Cells Failure

Bus bar between solar cells failure analysis is presented in Table 6

Table 6 Bus bar between solar cells failure analysis

Failure characteristics	Circuit disconnection
Causes	Defective connections
Features	Current absence
Effects	String failure
Effect Elimination	Non- recoverable
Criticality	Not allowed, it is permissible to have one string failure

The reliability of connection circuit depends on its constituent element reliability; the possibility of power bus line disconnection is about zero.

Points of welding failure analysis

The welding pints between the cells and each other at the power connection circuit block endings are tripled this way, so such circuit disconnection is possible only with the disconnection of more than three elements of one-type, and also it is permissible to have failure in one string so it is not considered as critical element [12].

Points of soldering and wires & Connection circuit failure

The reliability of connection circuit depends on its constituent element reliability; the possibility of power bus line disconnection is about zero.

The solders in connector contacts, cables, and connector contacts at the power connection circuit block endings are duplicated this way, so such circuit disconnection is possible only with the disconnection of more than three elements of one-type, the connections in SA systems like end-cap/body and end-cap/cable are duplicated, therefore, the circuit disconnections of any single element of SA power connection circuit do not lead to its disconnection; therefore, the power circuit is not critical.

The reliability of connection circuit is achieved by following the engineering discipline during the SA assemblage and by carrying out all types of SA tests, in this case the testing control is simplified by the fact, that the crippling of connection circuit (integrity of welded connections) is revealed easy enough [12].

In consideration of all these circumstances, and also extremely low possibility of connection circuit failure, it is possible to exclude the connection circuit from the list of the critical elements.

7. Engineering solutions for reliability assurance

As the made analysis shows, the solar array structure and control logic are such, that practically excluding the influence of any element failure at PSS operability.

The main structural solutions in this direction are following:

- 1- The application of the bypassing diode system for exception of the failed solar cell out of the circuit.
- 2- The Blocking block system for protect the strings.
- 3- Solar array control elements backup.
- 4- Electrical circuit duplication.

8. Solar arrays and photo voltaic Cells (SA&PVC) reliability calculations

In order to calculate the reliability of the system, the reliability diagrams must be first constructed according to components of the system reaching to the least level that can be reached or else the component will be considered as a closed box with a reliability value given from the subcontractor or manufacturer [2,4,15].

The essential elements of a reliability specification are:

- A quantitative statement of the reliability requirement specified by the customer as a minimum acceptable value.
- Environment of the power subsystem operation Mission lifetime in orbit and ground operation identification
- Constituted failure definition that should be expressed in terms which will be measurable during the demonstration test.

These elements were applied to the current system under the following conditions:

- The Satellite Power System (EPS) under study shall provide operation within 5 years of satellite active lifetime.
- The reliability of the EPS, within 5 years, shall be not less than 0.982.
- The EPS shall operate as specified under the following environments; 600 km altitude, ~63° inclination and AM0, temperature ~ (-40°C: +100 °C).
- The Satellite Power System (EPS) under study shall provide continuous operation within 5 years of satellite active lifetime.

From these diagrams the reliability equations are constructed according to the theory of operation of the system and the degree of redundancy required from each component.

Values of reliability of the different components are then substituted in the equations then reliability of the whole system is calculated and compared with the required reliability that must be achieved.

Reliability calculations are done after the FMECA is done in order to know the critical elements and places at which calculations are made and the feedback is put also in the FMECA [2].

Critical elements and places are those that cause the non-fulfillment of the requirements in the Technical specification.

Critical elements in the SA according to SA FMECA are [2,16]:

- 1- Solar cells;
- 2- Bus bar between solar cells;
- 3- Welding points;
- 4- Soldering points;
- 5- Integrated bypass diode;
- 6- Blocking device;
- 7- Wires.

Po ... Failure free operation

λ_i ... Failure rate of the element (1/hour)

Ti ... Period of operation

$$Q(\text{Failure}) = 1 - P(\text{Reliability})$$

These values of λ for each critical element and different operating conditions is obtained from the manual and passport of the element released by the manufacture of the element himself.

In order to perform the calculations, the reliability diagrams (Figures 3-5) must be constructed corresponding to the known level of reliability values known.

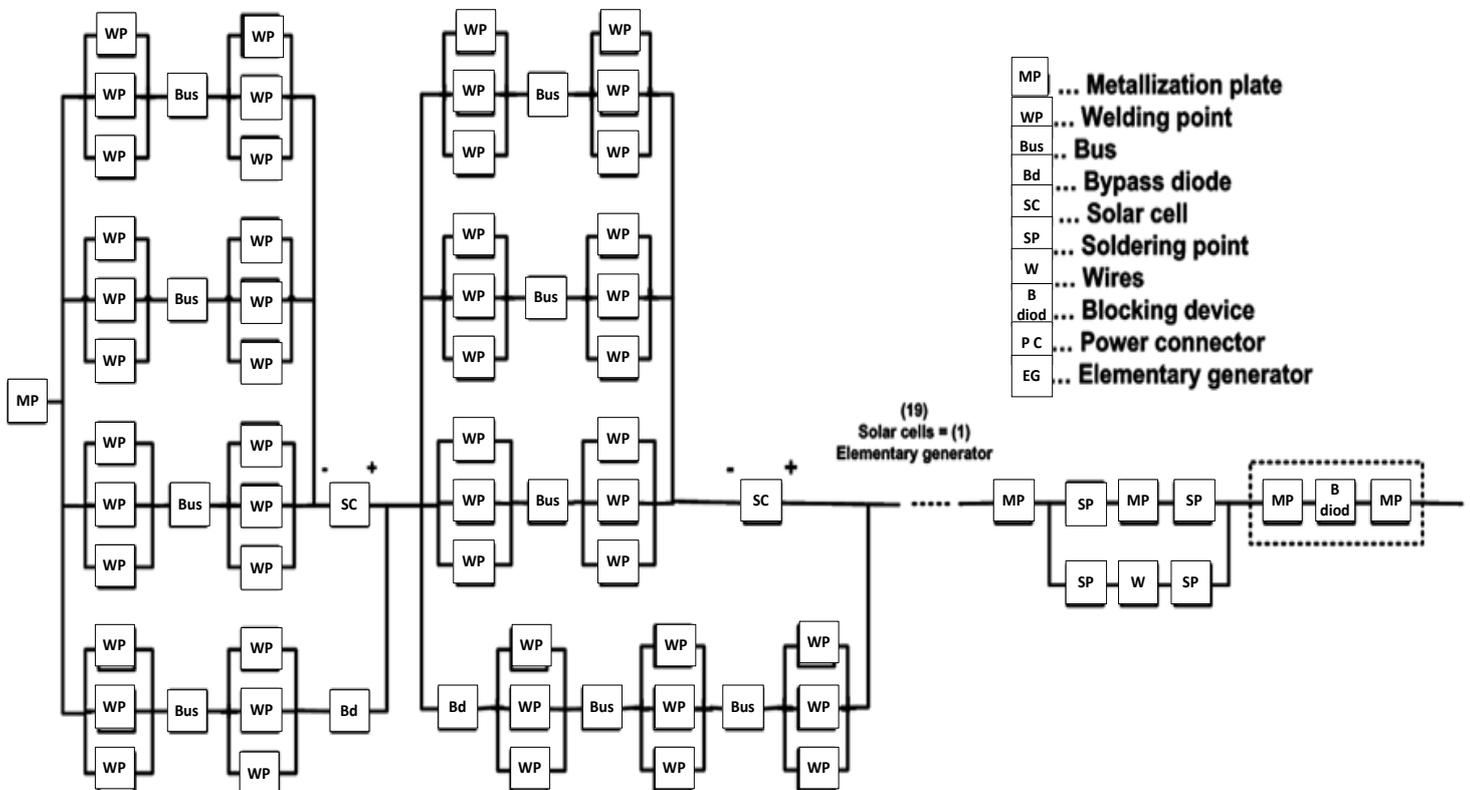


Figure 3. Reliability diagram for 1 elementary generator

In this diagram that is representing single elementary generator for the common LEO SC with Bus voltage of 28 V which considered the most common bus voltage for LEO SC, the level of the soldering points, welding points and wires is reached, each block in the diagram has specific reliability value corresponding to the manufacturing and the operating conditions during the whole life time.

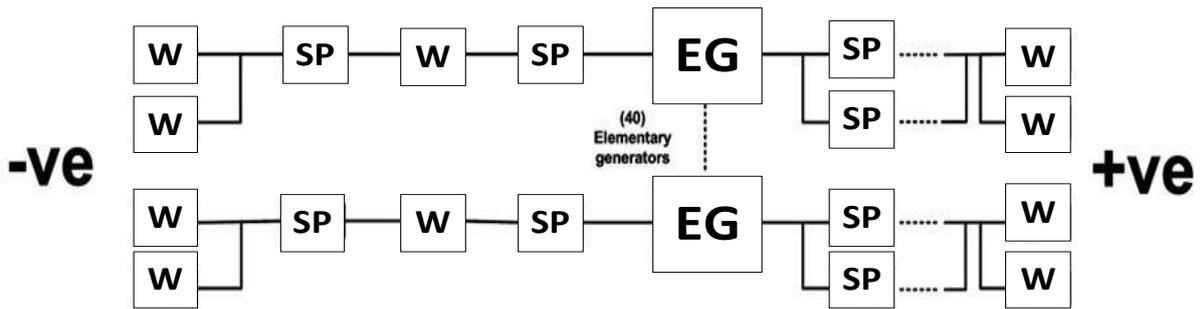


Figure 4. Reliability diagram for elementary generators (1 solar panel)

In this diagram, another level is reached containing the power connectors of the of the different elementary generators as an example for LEO SC solar array construction, the wires and soldering points between each elementary generator and its connector [14].

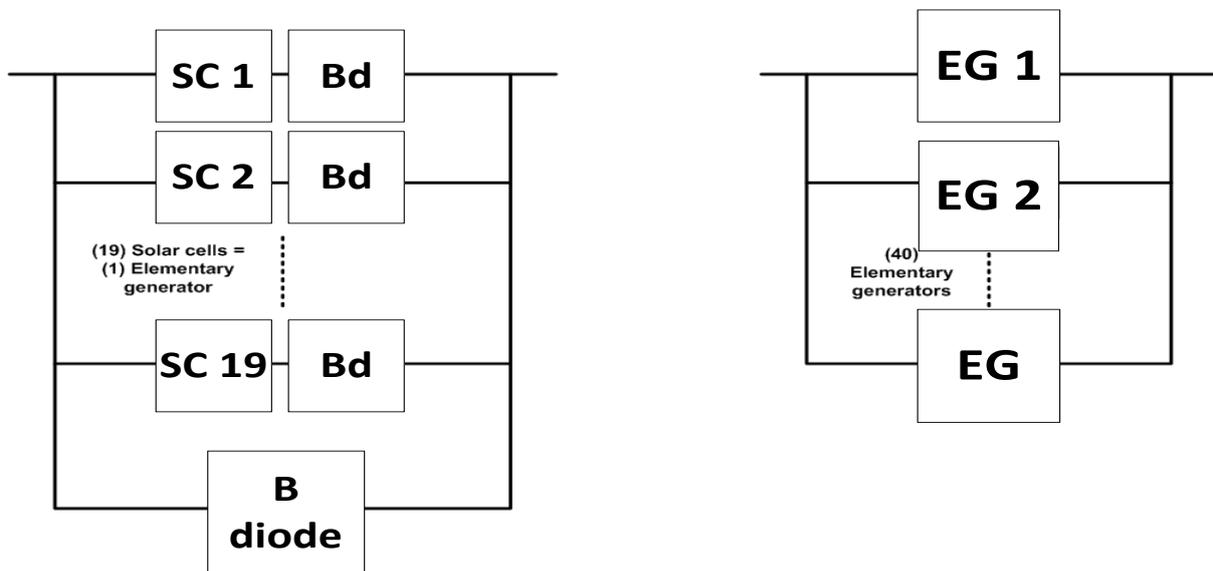


Figure 5. Reliability diagram of the solar panel as a whole

This general diagram for the solar panel is constructed after taking into consideration the reliability of the smaller details like welding points and wires into the reliability value of the shown blocks also after taking into consideration the reserve and redundancy degrees of the structure [2,17].

These values are then substituted in simpler reliability equation to get the reliability value of the whole solar panel and then for the 4 solar panels which is the reliability of the solar arrays and the photo voltaic batteries that will be included in the reliability calculations of the power supply system as a whole [14,15].

Reliability of the solar array and photo voltaic battery required according to spacecraft requirements [18] is 0.9982 and according to our FMECA analysis and the designed reliability scheme in the Design and the calculated it is not less than 0.9976.

Margins	5 years' life time
Margin of power	0.95
Margin of current	0.97
Margin of voltage	0.98

9. Conclusion

It is clear from our FMECA analysis that the whole critical elements in our solar array system is extracted and with the consequence of actions taken, the failure of any string is not critical, notably do not lead to the PSS failure or significant degradation.

According to the FMECA analysis the reliability scheme is created to ensure reduction of the risk of failure of the solar system by removing the criticality of the system elements.

10. References

- [1] ECSS-Q-30-02 Space product assurance - Failure modes, effect and criticality analysis (FMECA).
- [2] Space engineering Photovoltaic assemblies and components ECSS-E-20-08 Draft 4, 13 September 2007.
- [3] YACOV Y. HAIMES, RISK MODELING, ASSESSMENT, AND MANAGEMENT, Third Edition, Center for Risk Management of Engineering Systems, University of Virginia, Charlottesville, Virginia, WILEY.
- [4] Standard for Performing a Failure Mode and Effects Analysis (FMEA) and Establishing a Critical Items List (CIL) Flight Assurance Procedure (FAP) – 322 – 209.
- [5] MIL-STD-1629 Procedures for Performing a Failure Modes, Effects, and Criticality analysis.
- [6] GPR 7120.4A Risk Management.
- [7] ECSS-M-00-02A Space project management - Tailoring of space standards.
- [8] ECSS-Q-60 Space product assurance - Electrical, electronic and electromechanical (EEE) components.
- [9] Guide, Roland J. Duphily ‘Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA)’ ,Acquisition and Risk Planning Office , Mission Assurance Division , ,15 June 2009.
- [10] ISO 15387 1) Space Systems - Single junction space solar cells - Measurement and calibration procedures.
- [11] ECSS-Q-60-11 Space product assurance- EEE components -Derating and end-of-life parameter drifts.
- [12] ISO/CD 23038 1) Space systems - Space solar cells - Electron and proton irradiation test methods. [13]Patel, M. R., Spacecraft power systems, CRC Press, 2005.
- [13] ECSS-Q-70-08 Space product assurance - Manual soldering of high– reliability electrical connections.
- [14] ECSS-Q-70-26 Space product assurance- Crimping of high–reliability electrical connections.
- [15] ECSS-Q-20-07 Space product assurance - Quality assurance for test centers.
- [16] H. S. Rauschenbach, ‘Solar Cell Array Design Handbook’. New York: Van Nostrand Reinhold, 1980.
- [17] Guide, Roland J. Duphily ‘Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA)’ , Acquisition and Risk Planning Office, Mission Assurance Division, ,15 June 2009.
- [18] <https://directory.eoportal.org/web/eoportal/satellite-missions/p/pleiades>.