Space Transportation System Availability Requirement and Its Influencing Attributes Relationships

Russel E. Rhodes[1], Timothy C. Adams[2], and Carey M. McCleskey[3]
NASA, Kennedy Space Center, Florida, 32899

It is important that engineering and management accept the need for an availability requirement that is derived with its influencing attributes. It is the intent of this paper to provide the visibility of relationships of these major attribute drivers (variables) to each other and the resultant system inherent availability. Also important to provide bounds of the variables providing engineering the insight required to control the system's engineering solution, e.g., these influencing attributes become design requirements also. These variables will drive the need to provide integration of similar discipline functions or technology selection to allow control of the total parts count. The relationship of selecting a reliability requirement will place a constraint on parts count to achieve a given availability requirement or if allowed to increase the parts count will drive the system reliability requirement higher. They also provide the understanding for the relationship of mean repair time (or mean down time) to maintainability, e.g., accessibility for repair, and both the mean time between failure, e.g., reliability of hardware and availability. The concerns and importance of achieving a strong availability requirement is driven by the need for affordability, the choice of using the two launch solution for the single space application, or the need to control the spare parts count needed to support the long stay in either orbit or on the surface of the moon. Understanding the requirements before starting the architectural design concept will avoid considerable time and money required to iterate the design to meet the redesign and assessment process required to achieve the results required of the customer's space transportation system. In fact the impact to the schedule to being able to deliver the system that meets the customer's needs, goals, and objectives may cause the customer to compromise his desired operational goal and objectives resulting in considerable increased life cycle cost of the fielded space transportation system.

Nomenclature

A_i	=	inherent availability
MTBF	=	mean time between failure (hours)
MTTR	=	mean time to repair (hours)
λ	=	failure rate or the reciprocal of the MTBF
r	=	number of failures
N	=	total parts count
t	=	number of times the event is exposed

I. Introduction

IT is essential that management and engineering understand the need for a derived availability requirement for the customer's space transportation system. It is also essential to provide engineering and management the visibility of the several variables that determine availability required to enable the object's key goals and objectives. This

[1] AST, Technical Management, Engineering Directorate Design & Development Eng Div Sys Engineering & Integration Br, Kennedy Space Center, Florida/NE-D2, and AIAA Senior Member.

[2] AST, Reliability Engineer, Safety & Mission Assurance Directorate, Safety & Mission Assurance Integration Office, Integration Management Branch, SA-G2

[3] AST, Technical Management, Engineering Directorate Design & Development Eng Div Sys Engineering & Integration Br, Kennedy Space Center, Florida/NE-D2, and AIAA Senior Member.

relationship of the variables driving the availability capability needs must be understood by all decision makers involved. This paper will address the inherent availability which only addresses the mean downtime as that mean time to repair or the time to determine the failed article, remove it, install a replacement article and verify the functionality of the repaired system. Also with inherent availability the mean uptime will only consider the mean time between failures (other availability definitions consider this as mean time between maintenance – preventive and corrective maintenance) that requires the repair of the system to be functional. It is also essential that management and engineering understand all influencing attribute relationships to each other and to the resultant inherent availability requirement. Fig.1 provides a visual influence diagram of these attribute relationships to each other and to the resultant availability requirement. This visibility will provide the decision makers with the understanding necessary to place constraints on the design definition for the major drivers that will determine the inherent availability, safety, reliability, maintainability, and the life cycle cost of the fielded system provided the customer. This inherent availability requirement may be driven by the need to use a multiple launch approach to placing humans on the moon or the desire to control the number of spare parts required to support long stays in either orbit or on the surface of the moon or mars.

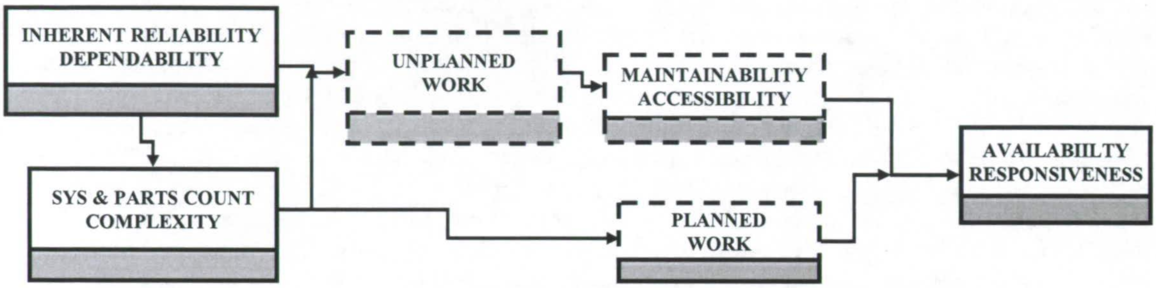

Figure 1. Availability influence diagram

II. Background

There are three types of availability, e.g., operational availability, achieved availability, or inherent availability. The basic definition of availability is equal to the mean uptime divided by the sum of the mean uptime plus the mean downtime. The major difference is the inclusiveness of the functions within the mean downtime and the mean uptime. The definitions of operational availability include the replacement hardware supply or maintenance delays and other non-design factors in the mean downtime. Also with inherent availability the mean uptime will only consider the mean time between failures (achieved availability definition considers this as mean time between maintenance – preventive and corrective maintenance that requires the repair of the system to be functional). For the purposes of this paper we will only be discussing inherent availability (A_i), Eq. 1,

$$A_i = MTBF / (MTBF + MTTR) \quad (1)$$

where MTBF is the mean time between failure and MTTR is the mean time to repair. MTBF is simply the time between any failures occurring in the system, e.g., the system no longer supports its intended function. MTTR is the total down time, e.g., that mean time to repair or the time to determine the failed article, remove it, install a replacement article and verify the functionality of the repaired system. Stating an availability requirement by itself will not accomplish the intended simple requirement. There are several major attribute drivers (variables) that influence or enable the achievement of the required availability. These major attributes are reliability, maintainability, and total parts count. This availability requirement and its influencing attributes must be developed together with them all becoming requirements. The relationship of these variables and the resultant achieved inherent availability must be understood by both engineering and management to enable the achievement of the customer's needs, goals and objectives.

III. Understanding the Availability and its Influencing Attributes Relationships

A. Defining Inherent Availability and its Influencing Attributes

We will address inherent availability from a design perspective. By emphasizing the importance of the key attributes that influence availability, we can control the need to perform unplanned work during long space missions or during the critical phases of the launch operation. Reliability or a metric of reliability (MTBF) by itself does not equate to availability. Availability is also influenced by maintainability or MTTR. As the reliability value of the system is increased the MTTR value becomes larger with a fixed availability requirement. Therefore, if the mission cannot accommodate the down time from a single failure from this projected MTTR requirement, there is a need for selecting a higher availability requirement. If the opposite approach is taken to reduce the reliability values desired to reduce the MTTR, then the projected number of failures would increase which requires more replacement parts, but resulting in the same total down time to maintain a working system. However, the total impact to the mission will be much greater, e.g., logistics impact from more parts failures and or the ability to provide the replacement parts when needed resulting in increased life cycle cost. Table 1 below illustrates this relationship between the requirements for MTTR and MTBF for different availability value requirements.

Table 1. Availability requirement as a function of system reliability requirement and mean time to repair requirement in hours and for a fixed mission time

Availability (A)

System Reliability	90%	94%	98%	99%	99.50%	99.90%	MTBF = -1/ln R
0.9500	2.17	1.24	0.40	0.20	0.10	0.02	19.496
0.9800	5.50	3.16	1.01	0.50	0.25	0.05	49.498
0.9900	11.06	6.35	2.03	1.01	0.50	0.10	99.499
0.9940	18.46	10.61	3.39	1.68	0.84	0.17	166.166
0.9950	22.17	12.73	4.07	2.02	1.00	0.20	199.500
0.9960	27.72	15.93	5.09	2.52	1.25	0.25	249.500
0.9980	55.50	31.88	10.19	5.05	2.51	0.50	499.500
0.9990	111.06	63.80	20.40	10.10	5.02	1.00	999.500
0.9998	555.50	319.12	102.03	50.50	25.12	5.00	4999.500
0.9999	1,111.06	638.27	204.07	101.01	50.25	10.01	9999.500

MTTR (Hours)

However, to understand the relationship of increased hardware failures to reduced reliability, we need to look at the probability of failures to total hardware parts count with respect to systems reliability. Poisson distribution can be used for predicting the number of failure events over a specific time. Eq. 2 is used to determine the probability of success of achieving the failure control desired. Fig. 2 and Table 2 illustrate this relationship of system complexity (parts count) to system reliability yielding the probability of success of controlling hardware failures by design.

$$\Pr = \sum_{n=0}^{r} \left[e^{-N\lambda t} \left(N\lambda t\right)^{n} / \left(n!\right) \right] \tag{2}$$

where using the "CUMULATIVE POISSON PROCESS" the probability of the number of failures can be projected. Where r is the number of failures, N is the total parts count, λ is the failure rate or reciprocal of the MTBF, t is the number of times the event is exposed and Pr is the probability of occurrence.

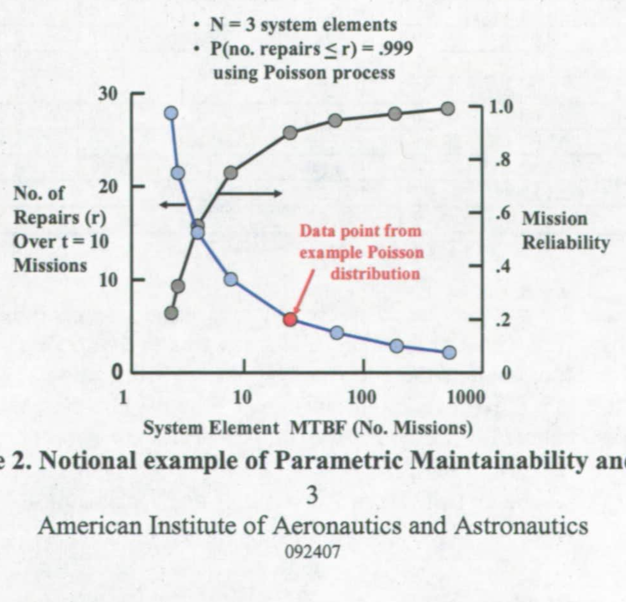

Figure 2. Notional example of Parametric Maintainability and Reliability Data

Table 2. System Complexity (parts count) shown as a function system reliability and probability of success of controlling failures to 1 or less per event in time

System Reliability(R)	MTBF = -1/ln R	System Complexity - Parts Count (N) Constraint: 20000	10000	2000	1000	500	100	50
0.9500	19.496	0.000%	0.000%	0.000%	0.000%	0.000%	3.629%	27.428%
0.9800	49.498	0.000%	0.000%	0.000%	0.000%	0.046%	40.055%	73.203%
0.9900	99.499	0.000%	0.000%	0.000%	0.048%	3.959%	73.391%	90.903%
0.9940	166.166	0.000%	0.000%	0.008%	1.708%	19.780%	87.750%	96.286%
0.9950	199.500	0.000%	0.000%	0.049%	4.001%	28.601%	90.942%	97.338%
0.9960	249.500	0.000%	0.000%	0.298%	9.099%	40.492%	93.823%	98.241%
0.9980	499.500	0.000%	0.000%	9.129%	40.546%	73.539%	98.244%	99.531%
0.9990	999.500	0.000%	0.050%	40.574%	73.557%	90.972%	99.532%	99.879%
0.9998	4999.500	9.155%	40.595%	93.844%	98.247%	99.532%	99.980%	99.995%
0.9999	9999.500	40.598%	73.574%	98.248%	99.532%	99.879%	99.995%	99.999%

Probability of Success for 1 or Less Parts Failing per Event

When evaluating total parts count, this can be considered in two different ways. If the concern is for affordability, the total parts count considers all components that could be considered to have a failure mode. Any parts failure will result in added maintenance burden and result in added life cycle cost. However, if the concern is for achieving a successful launch on time or for the in-space application for long term space flight, only the critical components (parts) should be considered that would impact the successful mission accomplishment. Because of this difference in objectives, the designer will probably want to perform both evaluations to allow the achievement of both objectives which can be controlled and accomplished by the design process. These attribute relationships and availability can be made more visible by examining scenario examples.

B. An example of Space Transportation Application

Let's work an example case through this process to allow better visibility of using these aids. Let's assume we will select a system with 0.999 system reliability and a desired availability of 98%, but the allowed MTTR if we experience a failure will only be allowed to be ~ 5 hours. We can easily see that the predicted MTTR for our example is 20.4 hours at this 98% availability; therefore, we must either select a higher availability or lesser system reliability. Using Table 3 we can see when using this 0.999 system reliability that the availability requirement needs to be adjusted to be 99.5% or better. The other option would be to select a lesser system reliability of 0.995 to retain this MTTR requirement of ~ 5 hours. If we were to make this lesser reliability selection, we need to determine the probability of experiencing hardware failures. Now it can be seen from Table 4 that the system complexity requirement would be constrained to ~ 50 parts count maximum at a 95% or better probability of success.

Table 3. Availability shown highlighted as a function of system reliability and mean time to repair in hours

System Reliability	Availability (A): 90%	94%	**98%**	99%	**99.50%**	99.90%	**99.99%**	MTBF = -1/ln R
0.9500	2.17	1.24	0.40	0.20	0.10	0.02	0.00	19.496
0.9800	5.50	3.16	1.01	0.50	0.25	0.05	0.00	49.498
0.9900	11.06	6.35	2.03	1.01	0.50	0.10	0.01	99.499
0.9940	18.46	10.61	3.39	1.68	0.84	0.17	0.02	166.166
0.9950	22.17	12.73	**4.07**	2.02	1.00	0.20	0.02	**199.500**
0.9960	27.72	15.93	5.09	2.52	1.25	0.25	0.02	249.500
0.9980	55.50	31.88	10.19	5.05	2.51	0.50	0.05	499.500
0.9990	111.06	63.80	**20.40**	10.10	**5.02**	1.00	0.10	**999.500**
0.9998	555.50	319.12	102.03	50.50	25.12	**5.00**	0.50	4999.500
0.9999	1,111.06	638.27	204.07	101.01	50.25	10.01	1.00	9999.500
0.99996	2,777.72	1,595.71	510.19	252.52	125.63	25.02	**2.50**	**24999.500**

MTTR (Hours)

Again it can be seen from Table 4 that it may be desirable to increase the systems reliability if it is unreasonable to constrain the parts count below 1000 with a probability of success greater than 95% (~ 98.25%). If we select a systems reliability of 0.9998 to accommodate the 1000 parts count, we will again need to adjust the availability requirement value to 99.9% to retain the MTTR requirement to ~ 5 hours; however, this assumes the time of the event is the full MTBF of ~ 5000 hours for the availability of 99.9% and the systems reliability of 0.9998.

Table 4. System Complexity (parts count) constraint example shown as a function of system reliability (0.999, 0995, & 0.9998) and 95% probability of success of controlling failures to 1 or less / event

Note: Red Font Cells in Row 6 & 7 are variables and can be changed to meet your application's needs.

Maximum number of failures = 1 or less (r) = 1 N*L*t

Failure rate of each system element (λ for Lambda) = - lnR and t = 1

A family of curves can be created for the Probability of Success for 1 or Less Parts failing per event with System Reliability Values of: (R) = 0.95 to 0.9999

System Complexity - Parts Count (N) Constraint

System Reliability(R)	MTBF = -1/ln R	5000	2000	1000	500	400	300	100	50
0.9500	19.496	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	3.629%	27.428%
0.9800	49.498	0.000%	0.000%	0.000%	0.046%	0.281%	1.647%	40.055%	73.203%
0.9900	99.499	0.000%	0.000%	0.048%	3.959%	9.011%	19.690%	73.391%	90.903%
0.9940	166.166	0.000%	0.008%	1.708%	19.780%	30.687%	46.123%	87.750%	96.286%
0.9950	199.500	0.000%	0.049%	4.001%	28.601%	40.465%	55.657%	90.942%	97.338%
0.9960	249.500	0.000%	0.298%	9.099%	40.492%	52.390%	66.176%	93.823%	98.241%
0.9980	499.500	0.049%	9.129%	40.546%	73.539%	80.850%	87.790%	98.244%	99.531%
0.9990	999.500	4.034%	40.574%	73.557%	90.972%	93.839%	96.303%	99.532%	99.879%
0.9998	4999.500	73.572%	93.844%	98.247%	99.532%	99.697%	99.827%	99.980%	99.995%
0.9999	9999.500	90.979%	98.248%	99.532%	99.879%	99.922%	99.956%	99.995%	99.999%

Probability of Success for 1 or Less Parts Failing per Event

For the purposes of determining the availability of the system, if the time of the event of interest is only the last 45 days (1080 hours) of the total MTBF of ~ 5,000 hours, we need to adjust the value for t in our model to 0.216 (the fraction of the MTBF). This 45 days target may represent a desired total time for receiving the hardware at the launch site, integrating the major elements, servicing the consumables, installing and connecting any ordinance, and launching the space transportation system into space. Visibility of evaluation for the 45 days can be seen in Table 5 where choosing a reliability of 0.995 (MTBF of ~ 200 hours) would restrict the parts count to ~ 300 with a probability of success of 95% or better where selecting the reliability at 0.9998 (MTBF of ~ 5,000 hours) would allow an excess of 5,000 total parts count and achieve a probability of success of having 1 or less failures during this 45 days of interest with a probability of success of 95% or better. Now that we have been working to achieve one or less failures, the design must accommodate this total repair time by providing accessibility during any part of the 45 days without any significant preparation. Experience has shown that hardware replacement that can be replaced in ~ a couple of hours before the vehicle is integrated, but if the failure occurs late in the launch pad servicing, the repair can take as much as 5 days because of the lack of accessibility for corrective action. With the availability requirement at 99.9% the MTTR requirement is ~ 5 hours as seen from Table 3.

Table 5. System Complexity (parts count) example shown as a function of system reliability (0.999, 0995, & 0.9998) and 95% probability of success of controlling failures to 1 or less per event in time; however, event time is reduced to only 45 days (1080 hours) of the total MTBF of ~ 5,000 hours.

Note: Red Font Cells in Row 5 & 6 are variables and can be changed to meet your application's needs.

Maximum number of failures = 1 or less (r) = 1 N*L*t

Failure rate of each system element (λ for Lambda) = - lnR and t= 0.216

A family of curves can be created for the Probability of Success for 1 or Less Parts failing per event with System Reliability Values of: (R) = 0.95 to 0.9999

System Complexity - Parts Count (N) Constraint

System Reliability (R)	MTBF = -1/ln R	20000	10000	5000	1000	500	400	300	100
0.9500	19.496	0.000%	0.000%	0.000%	0.019%	2.569%	6.460%	15.572%	69.612%
0.9800	49.498	0.000%	0.000%	0.000%	6.828%	35.901%	47.924%	62.359%	92.844%
0.9900	99.499	0.000%	0.000%	0.023%	36.173%	70.437%	78.404%	86.095%	97.958%
0.9940	166.166	0.000%	0.003%	1.128%	62.686%	86.139%	90.368%	94.112%	99.225%
0.9950	**199.500**	0.000%	0.023%	2.858%	70.537%	89.701%	92.936%	95.739%	99.455%
0.9960	249.500	0.000%	0.168%	7.026%	78.499%	92.942%	95.224%	97.158%	99.646%
0.9980	499.500	0.169%	7.051%	36.389%	92.955%	97.974%	98.666%	99.228%	99.909%
0.9990	**999.500**	7.063%	36.416%	70.616%	97.976%	99.457%	99.647%	99.799%	99.977%
0.9998	**4999.500**	78.559%	92.966%	97.977%	99.909%	99.977%	99.985%	99.992%	99.999%
0.9999	9999.500	92.966%	97.977%	99.457%	99.977%	99.994%	99.996%	99.998%	100.000%

Probability of Success for 1 or Less Parts Failing per Event

C. An example of long term In-Space Application

Let us now look at an example of long term exposure in space without the opportunity to provide re-supply of any hardware from earth. This might be considered as a trip to another planet like Mars where the trip time may be between two and three years. First we must choose a MTBF to accommodate the application such as ~ 25,000 hours (reliability of 0.99996). We can now see from Table 6 that the total parts count must be constrained to only 250 if we assume there are no failures allowed (Availability of 100%) and at a probability of success of 99% or 1,275 total parts count if we allow the probability of success to go to 95%.

Table 6. System Complexity (parts count) example shown as a function of system reliability at (0.99996) and 99% and 95% probability of success of controlling failures to 0 per event in time; however, the event time is long term in space of 2 to 3 years (~25,000 hours) or the total MTBF.

Note: Red Font Cells in Row 5 & 6 are variables and can be changed to meet your application's needs.

Maximum number of failures = 0 or less (r) = 0 N*L*t t = 1
Failure rate of each system element (λ for Lambda) = - lnR and t = 1

A family of curves can be created for the Probability of Success for 0 Parts failing per event with System Reliability Values of: (R) = 0.95 to 0.99996

System Complexity - Parts Count (N) Constraint

System Reliability(R)	MTBF = -1/ln R	5000	2000	1275	500	400	300	250	50
0.9500	19.496	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	7.694%
0.9800	49.498	0.000%	0.000%	0.000%	0.004%	0.031%	0.233%	0.640%	36.417%
0.9900	99.499	0.000%	0.000%	0.000%	0.657%	1.795%	4.904%	8.106%	60.501%
0.9940	166.166	0.000%	0.001%	0.047%	4.934%	9.006%	16.441%	22.212%	74.015%
0.9950	199.500	0.000%	0.004%	0.168%	8.157%	13.466%	22.229%	28.561%	77.831%
0.9980	499.500	0.004%	1.824%	7.788%	36.751%	44.897%	54.848%	60.623%	90.475%
0.9990	999.500	0.672%	13.520%	27.925%	60.638%	67.019%	74.071%	77.870%	95.121%
0.9998	4999.500	36.784%	67.029%	77.490%	90.483%	92.311%	94.176%	95.122%	99.005%
0.9999	9999.500	60.652%	81.872%	88.029%	95.123%	96.079%	97.044%	97.531%	99.501%
0.99996	24999.500	81.873%	92.311%	95.028%	98.020%	98.413%	98.807%	99.005%	99.800%

Probability of Success for 0 Parts Failing per Event

But if this application allows one failure to occur, it can be seen from Table 7 that the total part count constraint can be raised to ~ 3,700 at 99% probability of success or up to ~ 8,800 at 95% probability of success. The problem now becomes one of determining which hardware parts to take with this mission. Suggest the solution might be determined to take all 3,700 or 8,800 parts as spares to be sure to have the correct one.

Table 7. System Complexity (parts count) example shown as a function of system reliability at (0.99996) and 99% and 95% probability of success of controlling failures to 1 or less per event in time; however, the event time is long term in space of 2 to 3 years (~25,000 hours) or the total MTBF.

Note: Red Font Cells in Row 6 & 7 are variables and can be changed to meet your application's needs.

Maximum number of failures = 1 or less (r) = 1 N*L*t
Failure rate of each system element (λ for Lambda) = - lnR and t = 1

A family of curves can be created for the Probability of Success for 1 or Less Parts failing per event with System Reliability Values of: (R) = 0.95 to 0.99996

System Complexity - Parts Count (N) Constraint

System Reliability(R)	MTBF = -1/ln R	8800	5000	3700	1000	500	300	100	50
0.9500	19.496	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	3.629%	27.428%
0.9800	49.498	0.000%	0.000%	0.000%	0.000%	0.046%	1.647%	40.055%	73.203%
0.9900	99.499	0.000%	0.000%	0.000%	0.048%	3.959%	19.690%	73.391%	90.903%
0.9940	166.166	0.000%	0.000%	0.000%	1.708%	19.780%	46.123%	87.750%	96.286%
0.9950	199.500	0.000%	0.000%	0.000%	4.001%	28.601%	55.657%	90.942%	97.338%
0.9960	249.500	0.000%	0.000%	0.001%	9.099%	40.492%	66.176%	93.823%	98.241%
0.9980	499.500	0.000%	0.049%	0.510%	40.546%	73.539%	87.790%	98.244%	99.531%
0.9990	999.500	0.147%	4.034%	11.603%	73.557%	90.972%	96.303%	99.532%	99.879%
0.9998	4999.500	47.479%	73.572%	83.015%	98.247%	99.532%	99.827%	99.980%	99.995%
0.9999	9999.500	77.978%	90.979%	94.630%	99.532%	99.879%	99.956%	99.995%	99.999%
0.99996	24999.500	95.083%	98.248%	99.007%	99.922%	99.980%	99.993%	99.999%	100.000%

Probability of Success for 1 or Less Parts Failing per Event

Table 8 has been provided for additional visibility to allow for less total parts constraint. For this case four or less parts (selected) have been allowed to fail during the mission which allow the total parts count to increase to 31,000 with a probability of success of ~ 99% or 11,000 parts with a probability of success of ~ 99.99%. However, once again the problem is to determine which or how many spare parts to take along on the mission to be curtain to have the correct ones when needed (can we carry 31,000 or 11,000 spare parts?).

Table 8. System Complexity (parts count) example shown as a function of system reliability at (0.99996) and 99% and 95% probability of success of controlling failures to 4 or less per event in time; however, the event time is long term in space of 2 to 3 years (~25,000 hours) or the total MTBF.

Note: Red Font Cells in Row 5 & 6 are variables and can be changed to meet your application's needs.

Maximum number of failures = 4 or less (r) = 4 N*L*t

Failure rate of each system element (λ for Lambda) = - lnR and t = 1

A family of curves can be created for the Probability of Success for 4 or Less Parts failing per event with System Reliability Values of: (R) = 0.95 to 0.99996

System Complexity - Parts Count (N) Constraint

System Reliability(R)	MTBF = -1/ln R	31000	11000	2000	500	400	300	100	50
0.9500	19.496	0.000%	0.000%	0.000%	0.000%	0.001%	0.064%	41.810%	88.237%
0.9800	49.498	0.000%	0.000%	0.000%	2.739%	9.508%	27.700%	94.550%	99.618%
0.9900	99.499	0.000%	0.000%	0.002%	43.609%	62.490%	81.272%	99.626%	99.982%
0.9940	166.166	0.000%	0.000%	0.741%	81.374%	90.322%	96.320%	99.960%	99.998%
0.9950	199.500	0.000%	0.000%	2.878%	89.034%	94.689%	98.125%	99.983%	99.999%
0.9980	499.500	0.000%	0.000%	62.805%	99.632%	99.858%	99.960%	100.000%	100.000%
0.9990	999.500	0.000%	1.505%	94.726%	99.983%	99.994%	99.998%	100.000%	100.000%
0.9998	4999.500	25.910%	92.748%	99.994%	100.000%	100.000%	100.000%	100.000%	100.000%
0.9999	9999.500	79.816%	99.456%	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%
0.99996	24999.500	99.116%	99.990%	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%

Probability of Success for 4 or Less Parts Failing per Event

However, in these cases where parts are allowed to fail, the availability requirement becomes very important to ascertain the design has been constrained for accessibility and will permit parts replacement (MTTR) to be accomplished and in a timely manner. Table 3 will provide this needed visibility. It can be seen from this Table 3 that the Availability needed for this case would be 99.99% to constrain the MTTR requirement to 2.5 hours for this in-space repair to be reasonable.

IV. Conclusion

The availability requirement cannot be worked independently from the influencing attributes of MTBF requirement and MTTR requirement as well as a constraint on total parts count of the system being designed. These requirements must be developed together and maintained through out the design process with the understanding of all their relationships. If the design analysis capability discussed in this paper is used in the design, development, and evaluation (DDT&E) phase, the availability requirement, the MTTR requirement, the MTBF requirement, probability of success, affordability, and safety can all be controlled by design. However, because of there relationships to each other, they must be worked and developed together to provide the correct understanding and control to meet all of the objectives.

Additional benefits can be achieved by selecting the best technologies that provide major reductions in total parts count. Example would be to select a direct electro-mechanical control instead of using an intermediate fluid to perform the function while using the electro-mechanical device to control the intermediate fluid, e.g., electro-mechanical valve controlling fluid flow vs. a hydraulic or pneumatic operated valve while using a solenoid valve to control the hydraulic or pneumatic fluid which then controls the fluid valve. The use of common fluids for propulsion applications allowing an integrated system solution with only one fluid container would provide a major reduction in total parts count. When the criticality drives the design to provide redundant hardware solutions, the selection of hardware should always be at the best reliability possible to provide the lowest maintenance burden for lowering life cycle costs. In all of the above examples the resultant DDT&E and operational cost will be reduced along with the achievement of the highest overall system reliability and safety and can achieve a higher availability of the system enabling mission success.

In summary, added emphasis in any system development on the issue of inherent reliability, in so far as it addresses both parts count and MTBF, inevitably will improve performance, safety and operational affordability. Performance is improved when fewer, better parts are used as it should be the case these weigh less overall. Safety will be improved as hardware that fails less during checkout inevitably will perform better in actual use. Affordability is helped in each count as better performance makes each flight more productive or allows more flights given shorter process or production intervals. Ultimately hardware that can not be counted on to function during processing, regardless of redundancies, can not be expected to function well in flight. All that is lacking is the investment up-front, non-recurring that focuses on sufficient generic technology that numerous subsequent users can take advantage of to justify their initial investment, such as the example of selecting the best technologies mention above. But, this payback could be across the entire economic growth perspective and not limited to a single system use.

Acknowledgments

The author would like to acknowledge co-author, Tim Adams and Dr. Richard P. Heydorn of the Johnson Space Center for their technical support in identifying a means of balancing the requirements for safety, reliability, and maintainability where the use of the "Cumulative Poisson Process" should be used to predict hardware failure probability. Special thanks to several colleagues for their review and critique of this technical paper.

References

[1]Ned H. Criscrimagna, *Maintainability Toolkit*, IIT Research Institute, New York, 2000, pp. 43-46.

[2]Dr. Pat Odon, "Balancing Top-Level Space Transportation System Safety, Reliability and Maintainability Requirements, a tutorial" Space Propulsion Synergy Team Conference, Huntsville, Alabama, 2002, pp.13

[3]Dr. Paul Barringer & Associates, Inc., Web site http://www.barringer1.com, 8003 Pine Cup, Humble, TX, 77346-1740, USA