

N72-25980

**THE REDUCTION OF A "SAFETY CATASTROPHIC"  
POTENTIAL HAZARD - A CASE HISTORY**

by

**Joseph P. Jones**

**The Bendix Corporation  
Aerospace Systems Division**

**Presented at the**

**Second Government/Industry  
System Safety Conference  
Goddard Spaceflight Center  
Greenbelt, Maryland**

**May 27, 1971**

**PRECEDING PAGE BLANK NOT FILMED**

Early this year, the fundamental design concept of the Lunar Seismic Profiling (LSP) Experiment was challenged when a mode of operation on the lunar surface was identified which could conceivably result in the detonation of high explosive charges before the departure of the Apollo 17 astronauts. As a quantitative analysis of the problem was beyond our capability at the time and as the effects of an explosion on the lunar surface are unpredictable from a safety viewpoint, we found it necessary to report the problem to the Manned Spacecraft Center as potentially "Safety Catastrophic" as defined by NASA directive and by our own LSP System Safety Plan.

In this paper, I will attempt to track through the sequence of events, mainly as they relate to the system safety discipline, which resulted ultimately in the reduction of this potential hazard to "Safety Negligible." For the sake of brevity, I have minimized the discussion of the test results and some of the second order effects related to the operations of the hack watches.

The object of the LSP (Figure 1) is to utilize artificially induced seismic energy to investigate the physical characteristics of the lunar structure. It will be deployed on the surface of the moon during the Apollo 17 mission. Eight packages containing explosive materials ranging from 1/8 to 6 pounds will be set out at distances up to 3.5 kilometers from the Apollo Lunar Surface Experiments Package Central Station which will be erected near the Lunar Module. The packages are activated by the astronauts as they are set out by removing pull pins which initiate internal timing functions. (Figure 2)

From a safety viewpoint, the key components of each explosive package are the timers, two per package, which establish the conditions permitting the conversion of a firing command from the Central Station into the detonation of an explosive package after departure of the astronauts from the lunar surface. The timers are completely mechanical and each contains a modified military "hack" wrist watch movement which controls the advance of a timing drum to a position where the output function is initiated. The timers are preset and there are no controls or adjustments to be made during the mission. It remains only for the astronauts to remove

four pull pins to start the watch movements and to remove the mechanical, redundant in-flight safety features when the packages are in position on the lunar surface. (Figure 3).

When the safe/arm timer actuates, it moves a slide from a position in which it provides complete physical isolation of the end detonating cartridge (EDC) from the explosive block to a position in which a hole in the slide lines up to expose the explosive block to the EDC. This provides a propagation path to detonate the package. If for any reason detonation does not occur and the package is still intact after two hours, the timer will cause the firing hole to slide past the EDC, thereby permanently isolating the EDC from the explosive block.

One hour after the safe/arm timer opens the firing time window, the battery timer releases a firing pin which strikes a percussion primer in a thermal battery. The heat generated within the battery as a result of this action liquifies a normally solid material, creating an electrolyte which activates the battery for a period of approximately three minutes. With power applied to the receiver, decoder, and capacitive firing circuits, the explosive package is capable of responding to a firing command from the Central Station.

Early in the preliminary design phase of the timers, it was recognized that environmental conditions to which the watch movements would be exposed on the lunar surface would cause an increase in the amplitude of their balance wheels; this could cause "overbanking" and result in large timing errors and premature initiation of the timer functions.

The terms "balance wheel amplitude" and "overbanking" are fundamental to the problem and require a short description of the operation of a mechanical escapement watch movement (Figure 4) such as most of us still wear on our wrists. It should be made clear that tuning fork and quartz crystal regulated movements, which we all will see more and more or as time goes on, are not pertinent to this discussion.

Timekeeping in a watch movement is actually performed by controlling the rate of dissipation of energy from the coiled mainspring through a gear train. The control function is provided by the balance wheel and hairspring

assembly which, when properly adjusted, oscillates in simple harmonic motion. The timer hack watch, per common practice, oscillates at a rate of five times per second.

To define the terms previously mentioned, the measurement of angular displacement of a point on the rim of the balance wheel as it oscillates is the "amplitude" and is measured in "turns." The amplitude of a given watch movement is a function of its mainspring torque characteristics and is not adjustable. The maximum amplitude in any watch movement must be less than that which would cause the balance wheel to come around full swing and contact the escapement from the opposite direction. If this were to occur, the harmonic motion of the balance wheel would be disturbed by the rebound off the escapement and the rate would increase, causing the movement to run faster than normal. This condition, known as "overbanking," is never encountered in a normally operating watch here on Earth.

However, we have reason to suspect that astronaut wrist watches overbank. In an unofficial poll conducted at our request, when this problem first arose, most of the astronauts who were questioned responded that they noticed a tendency for their watches to run fast during a mission, and one was willing to estimate approximately plus twenty minutes per day. We might also note that, typically, the maximum possible amplitude of a fully-wound watch would be  $1\frac{3}{4}$  turns and the operating amplitude would be  $1\frac{1}{2}$  to  $1\frac{5}{8}$  turns with the balance wheel axis vertical (watch lying flat). With the watch on edge, the typical amplitude would be  $1\frac{1}{4}$  to  $1\frac{3}{8}$  turns due to increased balance staff pivot friction in this position.

In most instrument applications of watch movements, the primary concern is not the amplitude of the balance wheel but the rate of the watch; whether it runs fast or slow, and how much. The designer is free to allow the amplitude to fall within a rather large range as it has only a second order effect on rate.

In the LSP Timer, where safety and reliability are of the utmost importance, highly precise timing is the second-order requirement. We have determined that balance wheel amplitude, rather than rate, is the more important factor due to the unusually wide range of environmental factors under which the watch

is required to perform, and by the fact that there are upper and lower limits to usable watch amplitude.

The lower limit which we have not as yet discussed is not a precisely fixed point by an ill-defined area of poorer and poorer operation as the amplitude decreases. This is a condition which we earthbound people can relate to as this is exactly what happens to our watches when we fail to take them in for periodic cleaning. The lubricant gums up, the internal resistance of the mechanism increases, and, as there is no compensating increase in mainspring torque, less energy is transferred into the balance wheel and its amplitude decreases. This results in due course in noticeably large timing errors, erratic operation, and ultimately, inability of the watch to run at all. Low temperature has the same effect in that it causes the watch oil to congeal.

When the overbanking problem was originally presented to us by the timer subcontractor, they were unable or unwilling to predict the magnitude of the resulting timing error. They would only say that the watches could conceivably run "several times faster than normal". The main reason for this conservative approach probably was their total lack of quantitative information on the effect of the lunar gravity.

On our part, we had established a nominal 96-hour runout time requirement in order to maintain a 1.5 safety factor, or thirty hours, between the contingency lift-off time of the LM and the detonation of the first explosive package. We viewed any significant inroad on the safety margin with alarm and, for a time before we could put everything in proper perspective, were fearful that we did not have a viable design concept. The steps that we went through in getting to where we are today are noted in Figure 5. Each will be discussed briefly in turn.

The subcontractor had little difficulty in verifying that the problem was a real one. There was test experience from other programs to draw on which indicated that temperature and pressure were factors and the condition was demonstrable by the application of excessive torque to the mainsprings of randomly selected watches through their winding stems. You are all welcome to duplicate

this experiment on your own watches, but see your local watch maker, not me, if you shear off your winding stem.

I would like to show you at this point the form used to document this problem (Figure 6) within our program. Although the concept for the form and its format is my own, most of the checklist items are the work of Mr. J. Richey of Bellcomm, Inc., and were taken from a paper presented by him to the Washington Chapter of the System Safety Society on June 19, 1969. Normally, this form is used as a rough worksheet and has two purposes. First, it is intended to stimulate the imagination both of the System Safety Engineer and whomever he is trying to extract information on a problem. Second, it provides some kind of record of all the chaff we sift through in evaluating a problem, particularly the negative ones which are otherwise not documented. The form has been reasonably successful and has been adapted to other areas than manned spaceflight.

It seemed prudent, after overbanking was verified as a problem, to review alternate methods of providing the timing function for the LSP. Other methods had been considered and rejected in trade-off studies from which the selected design evolved. In the light of an overbanking problem of unknown magnitude, they might have appeared more attractive on second look. I won't belabor this effort, for all the potential candidates were still unattractive for various reasons, primarily weight and reliability. However, none could have scored as high on safety as the concept of two completely independent mechanical timers that could be initiated only by the astronauts during EVA. For once, the requirements of safety, weight, reliability, and volume were entirely compatible. We were convinced that we had the best design, if we could resolve the overbanking problem, and that a change at this point would guarantee nothing other than schedule slippage and cost overrun. We then chose to move on to the next step - to experimentally evaluate overbanking.

It was originally predicted that amplitude would increase on the moon because of high temperature, high vacuum, and low gravity. Experimental determination of the effects of temperature and pressure was a relatively

routine matter except for the necessity to adopt a state-of-the-art fiber optic instrumentation system to measure balance wheel amplitude to the order of accuracy required.

The real problem was in the evaluation of the effect of reduced gravity. It was known that balance wheel amplitude changes when the watch is changed from an edge position to a flat position because of changes in bearing friction. From this it could be inferred that the effect of gravity which would cause a similar change in bearing friction is not negligible and that a substantial increase in balance wheel amplitude over the nominal earth value could be expected when the watch was operating on the lunar surface. The question was, How much?

A centrifuge test was initially performed to provide g vs. amplitude data in the approximate range of 1 to 10 g and extrapolate backward to the lunar 1/6 g area. Not being convinced that this procedure was entirely valid, additional test methods were sought for cross-correlation.

As a result, two other methods were proposed - low or zero g flights in the C-135A aircraft operated by the United States Air Force as a zero g test and research facility and in the 500 foot free fall zero g research facility operated by the NASA Lewis Research Center. Tests were ultimately performed at both facilities under the sponsorship of the NASA Manned Spacecraft Center, the procuring agency for the LSP Experiment.

Although none of these three test approaches were in themselves completely conclusive, they all pointed in the same direction - that the increase in balance wheel amplitude under the influence of lunar gravity was no greater than one quarter turn. We thought at this point that we had the most important variable under control but, in fact, the most significant fact to be uncovered in the investigation was to come when the effects of pressure and temperature were investigated.

The results, of these tests as presented in Figure 7, substantiated the trend indicated in the initial tests, and a significant break point was found to exist in the 1 torr range. The maximum effect at 180° F, 1 torr, results in an increase in amplitude of approximately 1/4 turn. At the ambient temperature (approximately 75° F) only one of the three test

movements showed any appreciable change in amplitude (1/8 turn). However, beyond 1 torr the slopes increase sharply and in the hot case, extend into the overbanking region.

Another surprise was that our test results did not substantiate the traditional horological theory that aerodynamic damping significantly contributed to the total internal resistance of balance wheel system. This case had been so strongly made in our early discussions that a streamlined balance wheel was actively considered at one point as a partial solution to the overbanking problem. Although our data in the range of aerodynamic interest is scattered and somewhat questionable in an absolute sense, the general slope of the curve as it approaches 1 torr is unrefutable and indicated that the change of amplitude is less than that which an expert watch maker can observe.

The significant conclusion to be drawn from these tests is that, although maintenance of one atmosphere of pressure within the control module cavity is desirable for other reasons, non-catastrophic leak rates down to a minimum pressure of 1 torr during lunar operations have no great significance to the overbanking problem.

The results of holding pressure constant and varying temperature correlate. Two series of tests were performed, at ambient pressure and in the range of  $1 \times 10^{-4}$  torr. The summary results, corrected to eliminate torque variations due to mainspring wind down, are presented in Figure 8.

The effect of reduced pressure on the results of these tests are dramatic. Whereas a sharp point of inflection is displayed on the ambient curve in the 40-50° F range which renders amplitude essentially independent of temperature above this point, the vacuum curve rises steadily at a nearly constant rate and could cause a fully wound watch to overbank above 150° F. This is demonstrated by the points plotted above the 1 3/4 turn line, a physical impossibility as the balance wheel amplitude cannot increase beyond the point of overbanking. These points result from large corrections on measurements made after the vacuum chamber (and the watches) ran overnight to get down to test pressure. It may be inferred that, had the measurements been made immediately after winding the watches,

overbanking would have been observed in at least two of the test watches.

The close grouping of the data at the cold end of the curve suggests that pressure has little effect on amplitude at low temperatures but that there is almost a straight line relationship between temperature and amplitude in the range from stoppage at -35° F (-20° F in a vacuum) to the point of inflection at 40-50° F.

The final piece of information needed to evaluate the overbanking problem was related to mainspring torque characteristics. Mainsprings provide higher torque when fully wound up, and less as they run down. A characteristic torque curve is shown in Figure 9. The erratic torque variations at the high end of the curve are eliminated by the use of a recoil click in the winding ratchet mechanism which releases a few ratchet teeth before it locks the mainspring ratchet after winding. The low torque of the low end is eliminated by providing a longer mainspring run than is required for the mission involved. The resulting torque variations are thereby reduced to account for an amplitude variation of approximately one quarter of a turn.

Tests were conducted measuring torque as a function of mainspring wind as expressed in number of turns of the mainspring barrel. This information was used in correcting other test data to eliminate torque variation due to mainspring position, and to establish a representative slope, which turned out to be 4.4, to use in the presentation which follows. It should be mentioned here that the test watches used in this investigation were "set down" to a nominal one turn amplitude by substituting a convenient available mainspring from a smaller watch in the subcontractor's product line. The scope must be reverified in the 140 hour mainspring with which the production timers will be equipped.

Figure 10 shows the method by which the test results were put together to arrive at D and E conclusion that overbanking is not a matter of concern during normal operation of the LSP timer. Normal operation of course, means a condition in which seal integrity is maintained and the watches are operating at a nominal pressure greater than 1 Torr. As the O-Ring seals, three in number, constitute single point failures the next step was

to determine the worst resulting timing error on the safety of the astronauts and on the probability of success of the experiment.

This was accomplished by overbanking a watch under controlled conditions and measuring the resulting change in rate. By varying the controlled condition a curve was constructed of change as a function of overbank from which reliable predictions could be made. This curve is presented in Figure 11.

On the left side of Figure 11, it may be seen the application of a known torque to a fully wound down mainspring barrel resulted in the winding of the barrel to a point of equilibrium at which a certain balance wheel amplitude was attained. As the torque was increased incrementally, the barrel wound up further and the amplitude increased in a predictable manner. When the barrel was fully wound the amplitude continued to increase as a function of applied torque until the maximum amplitude was attained and the balance wheel overbanked. Up to this point there was no timing error measurable with a stop watch.

The curve continues on the right side of the figure but now, with the maximum amplitude attained and the watch running overbanked, the error rate becomes the dependent variable. Figure 12 repeats this portion of the curve as well as similar results for the other two test specimens.

As amplitude has thus been demonstrated to be a function of torque, the incremental increases in amplitude previously discussed can be converted to equivalent values of torque and, if combined in a rational manner, the resultant can be read out on the worst case curves in Figure 12 as a reasonable estimate of the worst timing error to be expected during lunar operations. This has been accomplished using graphical methods not discussed herein to account for the non-linearity of the torque curves in the overbanking range and to introduce a factor in the temperature effect based on the ratio of lunar gravity amplitude to earth gravity amplitude. Also accounted for and not previously discussed is the effect of an explosive package falling over on its side. After deployment the accumulative total of these worst case conditions is expressed as a maximum of 1750 grammillimeters of

equivalent torque which may be converted to a maximum error of +120 minutes per day.

However, the two watch movements in a LSP package are aligned in planes at right angles to each other and only one of the two timers will be lying flat when the package is lying on any side. Thus the overbanking condition would be applied to one of the two timers. This failsafe condition would tend to cause a dud rather than a premature explosion since the timers must both be within their respective time windows for the firing operation to function.

Therefore, considering only a total seal failure as the worst case on edge condition, the maximum torque value is approximately 1480 gram millimeters or an effort of plus 40 minutes per day. Ignoring the decrease in torque over 90 hours, this works out to approximately 10% of the established 30 hour safety margin, and is the basis on which the potential hazard has been reduced to "Safety Negligible."

Although the worst case approach has sufficed to resolve our safety concerns, it does little to resolve the residual reliability problems. We are now at work developing a mathematical model of the balance wheel system to which we can apply our test results and predicted mission time line data to permit more meaningful analysis closer to the real case conditions which will actually exist. The O-Ring seal design is also under rigorous review at this time as a result of this investigation.

The remaining system safety task to be performed is indicated in Figure 13, which will ultimately become part of the safety assessment report for the LSP Experiment. We must establish the maximum torque and the slope of the production mainspring torque curve to assure lunar operation conforming to that presented in Figure 10. It is now important to establish tolerances on these numbers which will assure safe and reliable performance of the LSP experiment yet will have an impact on production costs and schedules no greater than required to achieve this goal. This is the sometimes forgotten system safety task which can not be overlooked in our ever more competitive industry. The system safety

engineer must be as cost conscious as all the other engineering disciplines and must see to it that no more effort is being expended in the name of safety than is necessary to achieve the desired results.

In closing, I would like to express my appreciation to several people; to Mr. Charles A. Sauter of the Bulova Watch Company and Mr. Rene' Besson of Ebauches S.A., (Neucha-

tel, Switzerland); to Mr. Jack Dye, The LSP Experiment Manager, without whose encouragement I would not be here; to Mr. Donald G. Wiseman, Manager of the Lunar Surface Project Office at the Manned Spacecraft Center for Authorizing the presentation of this material and to Bill Scarborough, who bears the responsibility for me being a System Safety Engineer.

**DEPLOYED LAYOUT**

3.5 KM MAX

3.5 KM MAX

3.5 KM MAX

8 EXPLOSIVE PACKAGES DEPLOYED ON 2ND & 3RD LAY TRAVERSE

180°

150°

120°

90°

300°

330°

30°

400' 300' 200' 100' 0' 100' 200' 300' 400'

FOUR GEOPHONES DEPLOYED IN TRIANGULAR ARRAY

ALIAS CENTRAL STATION

LINK TO BE CUT AT INSTANT OF DETONATION

Thermal Battery Timer

Receiver & Signal Processor

Thermal Battery

Firing Pulse Generator

Test Connector

Pull Pin (4)

Sale Arm Slide Assy

High Explosive B.A. Assy

End Disruptive Cartridge

Handset

2

EP

Rotary Antenna

Slide Position Indicator

Slide Arm Slide Timer

Sliding Plug

The diagram illustrates the timing system for the Apollo 11 lunar module. It shows the electrical connections between the Astronaut Pull Rings (No. 1, 2, 3), the Timing Mechanism, the Firing Pin Mechanism, the Thermal Battery (W/Primer), the Receiver, the Signal Processor, the Firing Pulse Generators, and the End Detonating Cartridge. It also shows the connection to the LSP Transmitter for RF Commands. The diagram includes a cross-section of the lunar module structure showing the Safe-Arm Plate, HNS Load, and H.E. Charge. The timing sequence is defined by  $T_D$  (Astronaut Pull Rings Removed at Deployment) and  $T_N$  ( $T_D$  + Pre-set Time, 90, 91, 92, or 93 hours).

**Legend:**

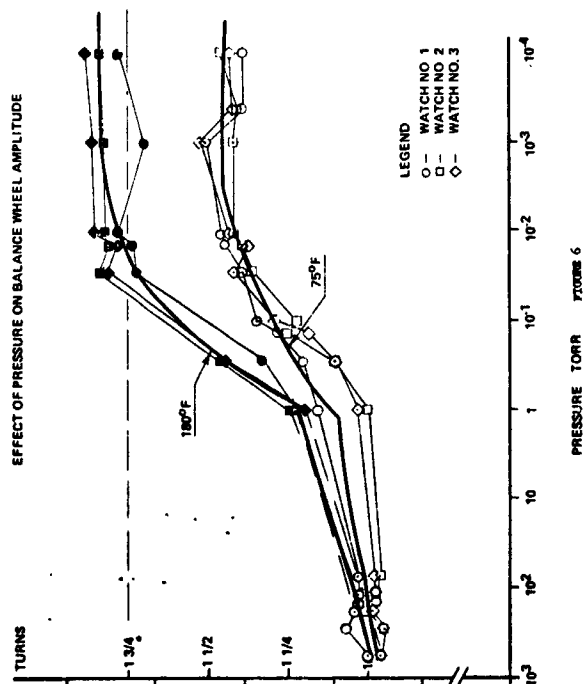
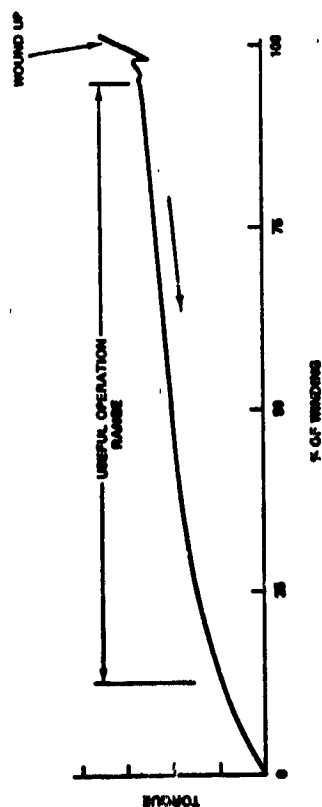
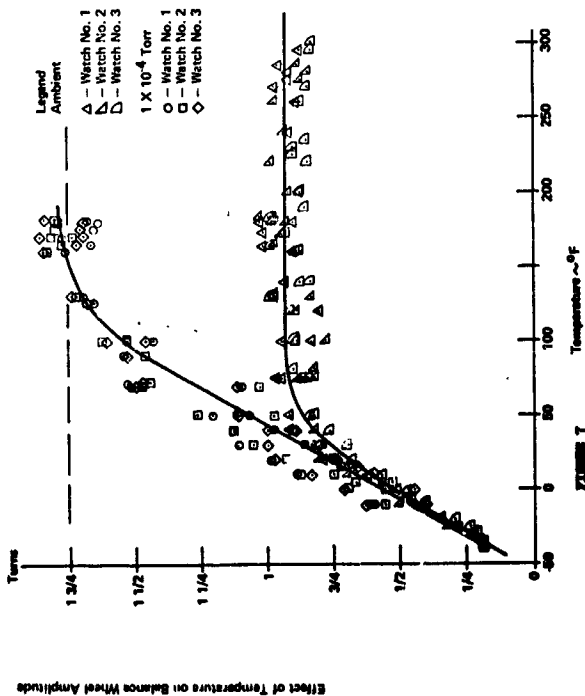
- $T_D$  = Astronaut Pull Rings Removed at Deployment
- $T_N = T_D + \text{Pre-set Time (90, 91, 92, or 93 hours)}$


**Labels in Diagram:**

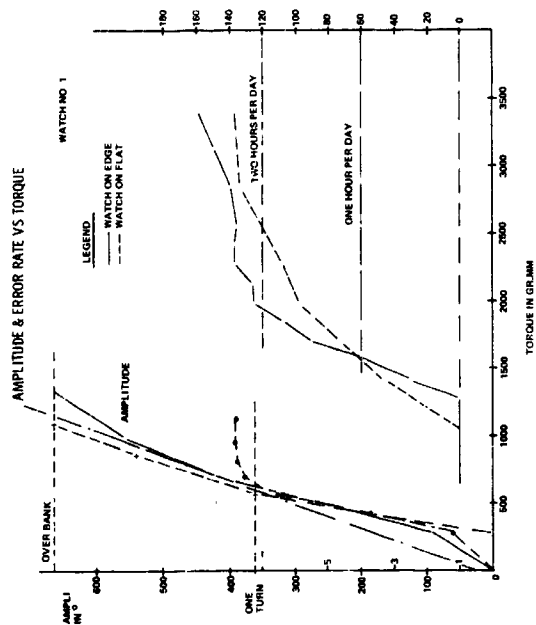
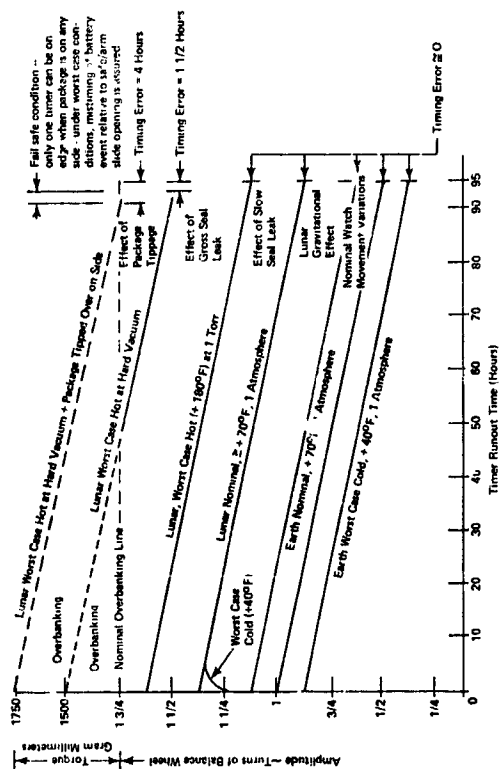
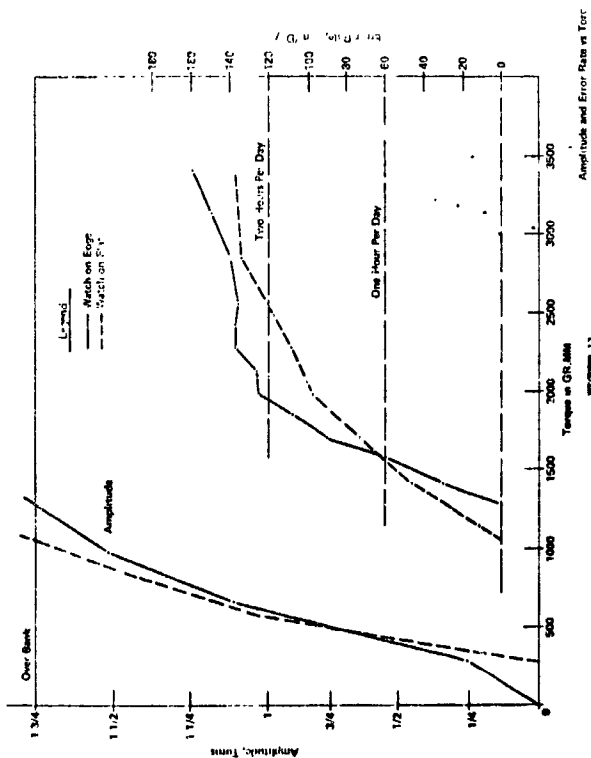
- Astronaut Pull Ring No. 3
- Timing Mechanism
- Firing Pin Mechanism
- Thermal Battery (W/Primer) (2 min life)
- LSP Transmitter RF Commands
- Receiver
- Signal Processor
- Firing Pulse Generators
- End Detonating Cartridge
- Tension Spring
- Safe-Arm Plate
- HNS Load
- H.E. Charge
- Astronaut Pull Ring No. 1
- Astronaut Pull Ring No. 2
- Timer No. 1
- Timer No. 2
- Open -  $T_N$
- Close -  $T_N + 2 \text{ hrs}$
- $T_N + 1 \text{ hr}$
- $+24 \text{ VDC}$
- $+5 \text{ VDC}$
- $+13 \text{ VDC}$
- $T_N + 1 \text{ hour} + 2 \text{ min (max) (RF Command)}$

202





 <b>Boeing</b> Aerospace Systems Division	Date: 1-25-71 By: [Signature] Title: LSP Name: J. Jones	
	<b>SYSTEM SAFETY PROBLEM SHEET</b> WATCH MOVEMENTS IN F&S/A THREATS	
Watch Movements may "overlook" and run several times faster than normal under linear environmental conditions of temperature, vacuum, and gravity.		
Possible/suspected/suspect event. Arming and power conditions may be satisfied prior to scheduled occurrence of firing event. The transmission of a firing command control station in LSP model would cause a premature detonation, possibly before departure of LSP.		
1. IMPROPERLY CALIBRATED MOVEMENTS 2. IMPROPERLY CALIBRATED MOVEMENTS 3. IMPROPERLY CALIBRATED MOVEMENTS 4. IMPROPERLY CALIBRATED MOVEMENTS 5. IMPROPERLY CALIBRATED MOVEMENTS 6. IMPROPERLY CALIBRATED MOVEMENTS 7. IMPROPERLY CALIBRATED MOVEMENTS 8. IMPROPERLY CALIBRATED MOVEMENTS 9. IMPROPERLY CALIBRATED MOVEMENTS 10. IMPROPERLY CALIBRATED MOVEMENTS	High initial bounce wheel amplitude typical of good Earth practice would not permit increase in "linear" environment without overloading.	
Overloading causes failure to run fast and to prematurely satisfy explosive package firing conditions.		
Effect of premature detonation and predictable. The worst case of misoperation of the event and/or the LSP must be considered.		
Neither crew nor Mission Control can monitor timer performance and would not be aware of the fact that a timer overhauled.		
LSP Mission compromised by loss of one or more of eight explosive packages. If a timer does not fire, a timer could still result in post detonation data depending on circumstances.		

[illegible]