D/0

N84 25088

INHERENT PROBLEMS IN DESIGNING TWO-FAILURE TOLERANT ELECTROMECHANICAL ACTUATORS

Stephen Hornyak*

ABSTRACT

An electromechanical ac-powered rotary actuated four-bar linkage system for rotating the Shuttle/Centaur deployment adapter is described. The essential features of the deployment adapter rotation system (DARS) are increased reliability for mission success and maximum practical hazard control for safety. This paper highlights the requirements, concept development, hardware configuration, quality assurance provisions, and techniques used to meet two-fault tolerance requirements. It presents the rationale used to achieve a degree of safety equivalent of that of two-failure tolerance. Conditions that make this approach acceptable, including single failure point components with regard to redundancy versus credibility of failure modes, are also discussed.

INTRODUCTION

During the last 3 years, a NASA/DOD agreement led to the design, development, and procurement of the Centaur G-prime and Centaur G high performance upper stages. The configuration is derived from the flight-proven Atlas/Centaur and Titan/Centaur vehicles. The Centaur G-prime is a NASA-unique version of the configuration that will launch the Galileo and International Solar Polar (ISPM) spacecraft. The Centaur G will carry and eject DOD-unique satellites into geostationary or 12-hour orbits. The Centaur spacecraft will fly as a dedicated Shuttle payload. Integration of the Centaur upper stage into the Orbiter is accomplished by using the Centaur integrated support system (CISS), consisting of the Centaur support structure (CSS); deployment adapter (DA); and the associated CISS electronics, fluid, and mechanical systems. An overview of the Shuttle/Centaur configuration is illustrated in Figure 1.

The DARS is part of the CISS mechanical systems and performs the DA rotation function for both Centaur G-prime and Centaur G upper stages. This paper describes the rotation system designed for G-prime and discusses possible changes for the G version.

The DARS is required to provide reliable DA positioning for Centaur separation and deployment, to react primary reaction control system (PRCS) jet moments during the erected position without latches, and to return the Centaur safely back to the stowed position in case of an aborted mission. Following a successful Centaur ejection from the Orbiter cargo bay, the function of the DARS is to rotate the empty DA back to the stowed position and restrain it for Orbiter landing. Independent single-failure tolerant primary and backup rotators are used in combination to guarantee the effect of two-failure tolerance. The rotation system is fail-safe in that two failures will not lead

* General Dynamics Convair Division, San Diego, California

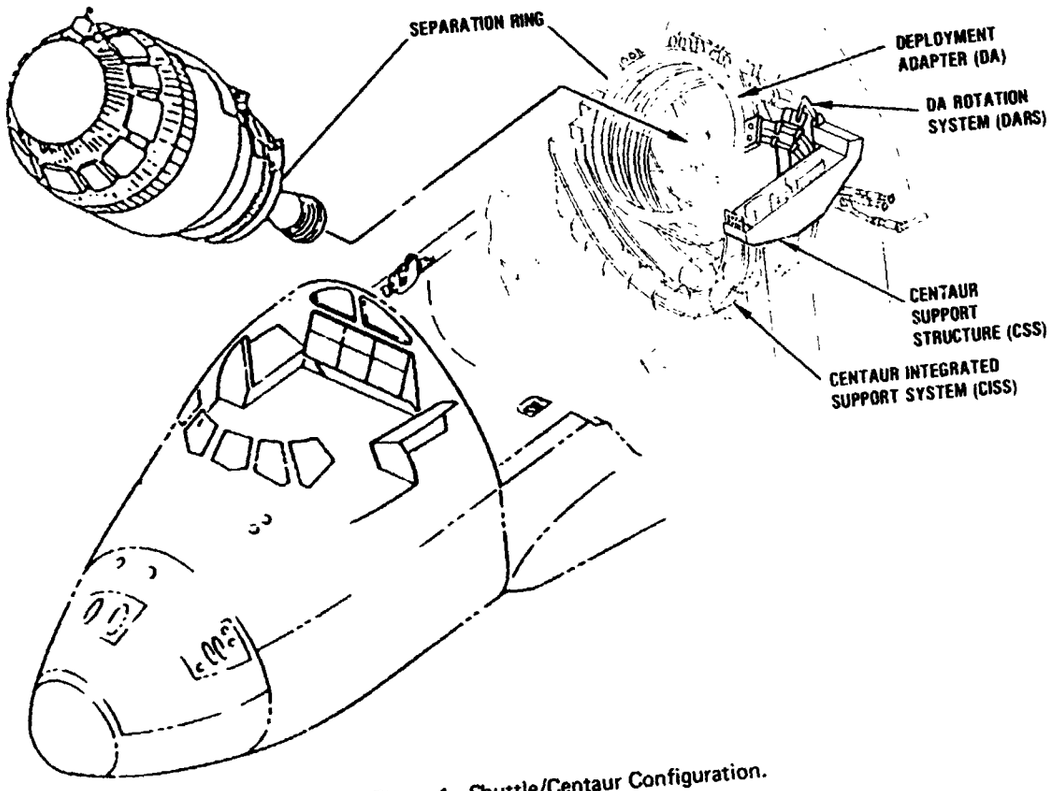

Figure 1. Shuttle/Centaur Configuration.

to catastrophic hazard. Manual disengagement capability of the link, for contingency only, is provided with the use of crew trained EVA (extra vehicular activity) to free a jammed rotator in orbit.

The Centaur spacecraft can be then returned to the stowed position using the contingency EVA winch (designed to restow the IUS manually) which is a slightly modified version of the contingency payload bay door winch mounted on the Orbiter forward bulkhead.

The relationship between DARS and CISS is shown in Figures 2 and 3. The DARS and the systems interfacing with DARS are shown in block diagram form in Figure 4.

The concept, the requirements, and the procurement specification of the mechanisms described in this paper were developed by General Dynamics, which subcontracted the electromechanical rotator unit design, manufacturing, and testing to the Hoover Electric Company.

REQUIREMENTS

The requirements imposed on the rotator to perform several functions within severe constraints are summarized as follows:

Safety Requirements (in accordance with NHB 1700.7A)

- Independent primary and backup rotation methods are required.
- Combination of primary and backup methods must be two-failure tolerant.

Operational Requirements (in accordance with JSC-07700 Volume X, Appendix 10.16, September 30, 1983)

- Erect Centaur to 36° minimum, 45° maximum rotation angle for Centaur separation.
- Erection capability required under active vernier reaction control system (VRCS) or free drift conditions (PRCS and Orbiter maneuvering system (OMS) translation modes inhibited during rotation).
- Capability required to react VRCS and PRCS loads while Centaur is in the erected position.
- Orbiter/CCE (Centaur cargo element) dynamic interactions shall be minimized.
- Multiple (up to six) erection/restow cycles anticipated for each mission; restow capability for abortive missions is required.
- Performance is required through 10 Orbiter missions over 10 years.
- Fatigue life must be designed to four times the expected number of mission cycles.
- Redundancy verification is required during turnaround.

System Requirements (derived, assumed, or self imposed)

- Rotate DA to 45° in 4 to 5 minutes.
- Operation is required in both one g and zero g conditions.
- Disengage the crank clutches of both primary and backup rotators during ascent and reentry (in case of an aborted mission).

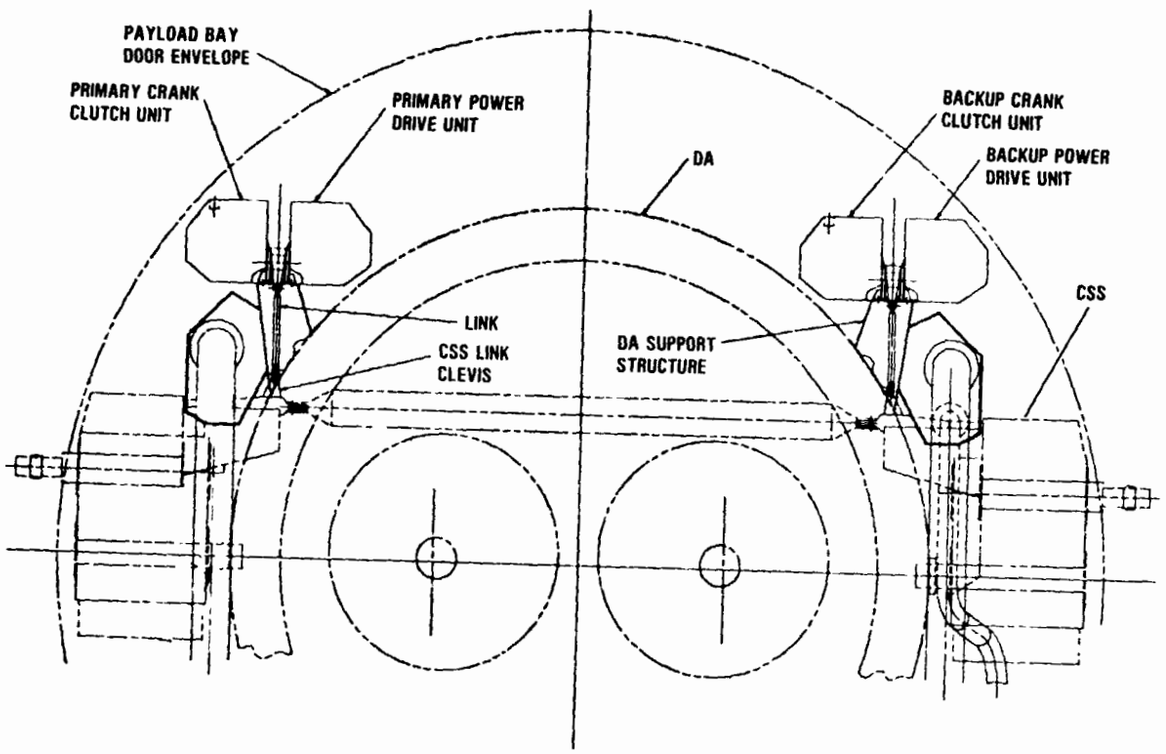

Figure 2. DA Rotation System Configuration (Rear View).

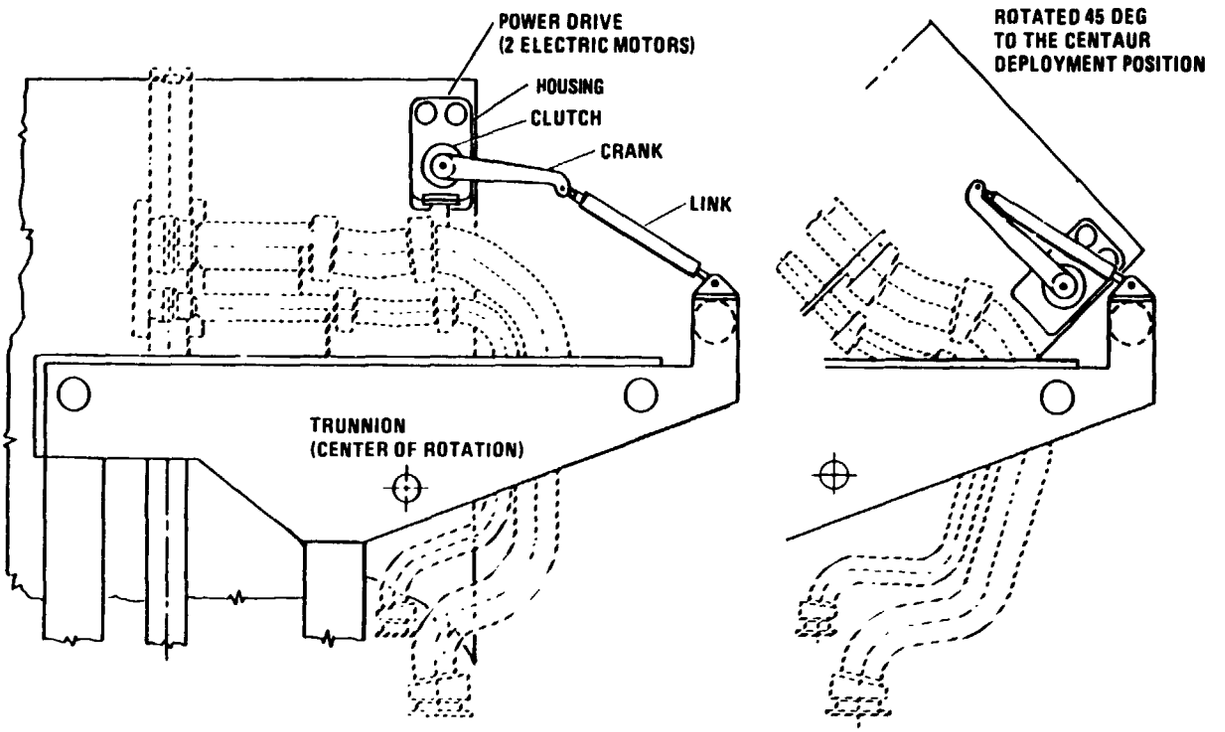

Figure 3. DA Rotation System Configuration (Left-Hand Side View).

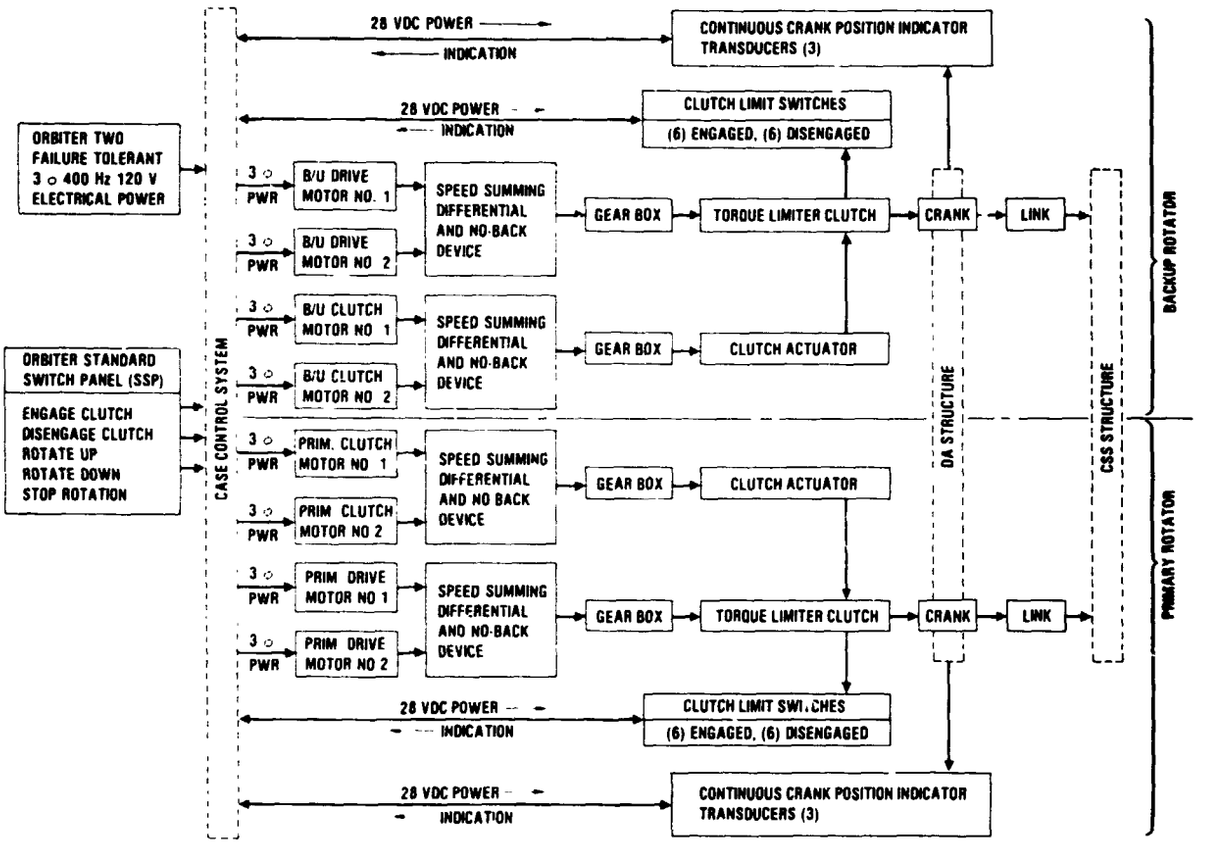

Figure 4. DA Rotation System (Functional Block Diagram).

- Only one of the clutch or rotation motors shall operate at a time.
- Weight shall not exceed 310N (70 lb) per rotator.
- Operation is required at temperature extremes from - 73° to 121°C (- 100 F to 250 F).
- The rotator must perform after exposure to severe vibroacoustic environments during Shuttle ascent to orbit, with special consideration for its installed position on the structural support extending from the aft ring of the DA.
- After a successful Centaur separation, the DA shall be returned to the reentry position 0.5° beyond the nominal stowed position of Centaur and preloaded against a stop using both rotators to react Orbiter landing loads safely.
- DA in any position must not violate the payload bay door envelope.
- Limit switches, crank position transducers, ac power, and avionics shall be two-failure tolerant.
- Software/Control requirements are:
  a. Automatic rotation operation after crew initiation.
  b. Automatic failure detection and reconfiguration.
  c. Orbiter signals are not required for operation.
- Ground checkout requirements are:
  a. One rotator to cycle DA with CSS in horizontal position.
  b. One rotator to cycle counterweighted DA with CSS in vertical position.
- Existing space technology (manufacturing and testing) developed for electromechanical rotary actuators employed in the Orbiter and other similar space applications shall be used as applicable in the rotation system design.

CONCEPT DEVELOPMENT

During the design selection phase, most of the problems centered around the two-failure tolerance requirement. Many different designs were conceived and eliminated in tradeoffs. Rack and pinion, ballscrew, chain, cable, and steel-belt drives — employing one or a combination of hydraulic, pneumatic, electrical, and pyrotechnically powered actuators — were evaluated against linkage drives. The linkage drive was selected for this application based on its excellent kinematic behavior. This electromechanical quadric crank mechanism concept, which uses reliable technology already developed and tested for similar applications in the Orbiter, ensures trouble-free performance and avoids the costly development usually associated with an innovative design and the inherent risks associated with meeting tight schedules.

HARDWARE CONFIGURATION

One DA rotator, illustrated in Figure 5, consists of the following major components.

A. Rotary actuator, including the following subassemblies:
   (1) Power drive unit – a rotary electromechanical device consisting of two input channels driving a rotary output shaft through a reduction gearing arrangement that provides for independent operation of each input channel. The two input channels will not be operated

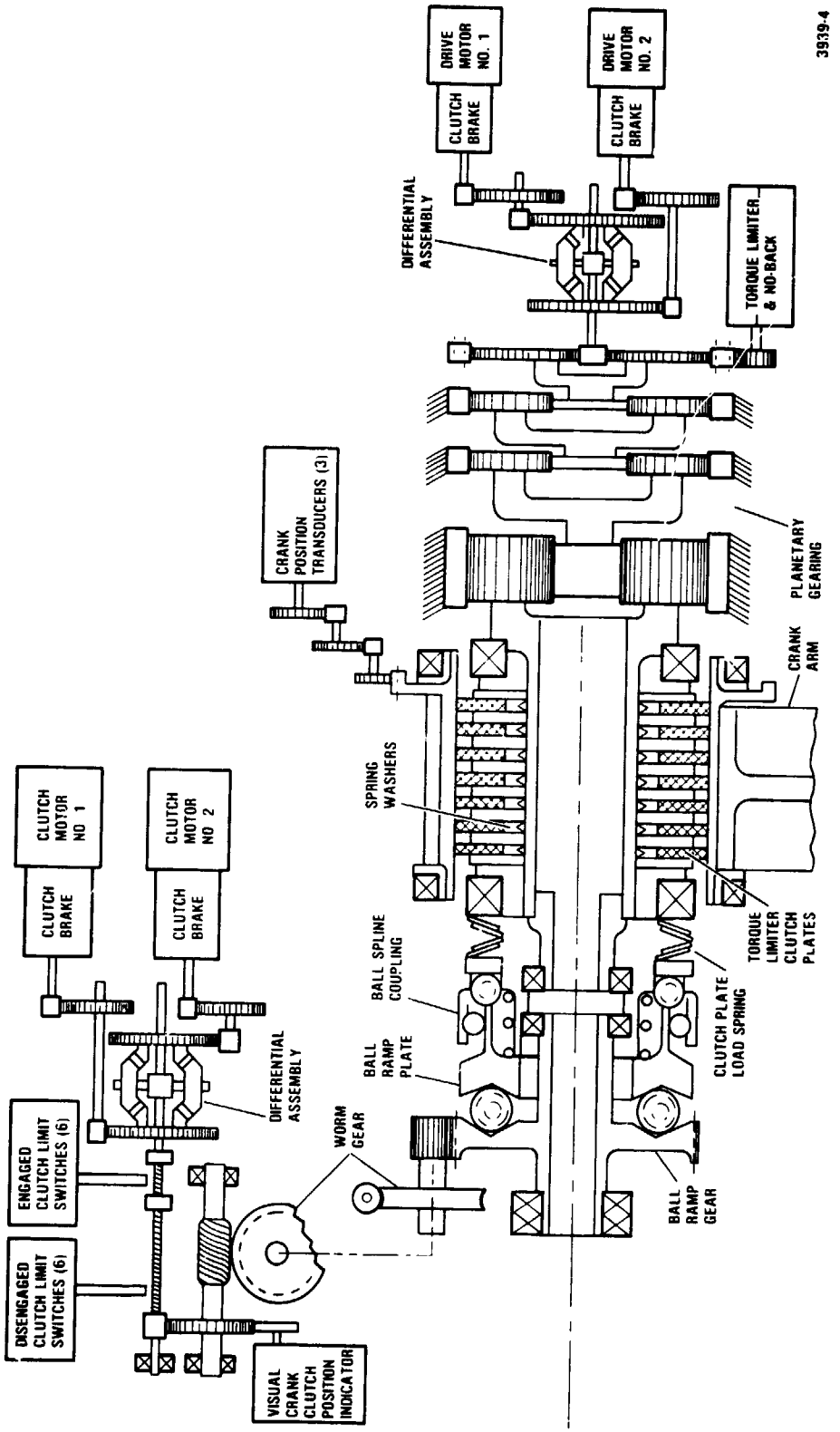

Figure 5. DA Rotator Component Arrangement (Schematic).

concurrently. Failure of any one channel will not affect operation of the remaining channel. The power drive unit output torque will meet the requirements with either channel operating.

(2) Crank clutch unit — actuated by an electromechanical device similar to the power drive unit. The clutch will transmit the output shaft torque of the power drive unit into the crank shaft. The power drive clutch is located between the output shaft of the unit and the crank shaft. Limit switches are used to indicate engaged and disengaged clutch positions. The clutch also serves as a torque limiter, protecting the rotator and the interfacing structure from overloads.

(3) Crank — transforms crank shaft torque into force in the link. Electrical rotary position transducers are used to indicate continuous crank position.

(4) Housing — supports the crank shaft, power drive unit, and crank clutch unit. It is capable of withstanding the full crank load and maximum vibration loads while bolted rigidly to the housing support structure on the DA.

B. Link — The link is pushed/pulled by the crank arm and transfers crank output into deployment adapter position. The link has two self-aligning rod end bearings and is pinned to the CSS-mounted clevis.

The rotator is designed to perform the required functions under the following conditions:

- The available power is two-failure tolerant Orbiter 400 Hz 115/200 vac, three-phase, four-wire for motors and 28 Vdc for limit switches and transducers.
- The two drive motors and the two clutch motors are identical, and each motor operates independently. Failure of a motor or a power failure to that motor will be followed by switching off the disabled motor and switching on the second motor to complete the function. The deenergized motor does not interfere with the performance of its twin motor. Each is rated to perform under the worst-case combination of temperature, altitude, voltage, frequency, and loads.
- Operating time is 45° rotation in 4 to 5 minutes.
- Loads are divided into four catagories. The crank torque limit values are as follows:

(1) Operating in orbit–520 Nm (4,600 in-lb)

(2) PRCS jet moments–2,940 to 4,070 Nm (26,000 to 36,000 in-lb)

(3) Landing–2,920 Nm (25,800 in-lb) reacted by two rotators

(4) Ground checkout–570 Nm (5,000 in-lb

- Maximum slip torque at crank shaft–4,070 Nm (36,000 in-lb).
  Minimum transmission torque at crank shaft–2,940 Nm (26,000 in-lb).
- Rotator overall stiffness–113,000 Nm (1.0×10^6 in-lb) per radian minimum spring rate in the direction of crank rotation, measured at the center of the rotator mounting plate.
- Position transducers: Crank rotation between mechanical stops is monitored by three position transducers per rotator. A group of five transducers will be used simultaneously, combining the primary and backup rotator transducers, to meet two-failure tolerant signal control criteria for Centaur positions, ensuring a three-versus-two vote by avionics in the worst-case condition. The sixth transducer is reserved for instrumentation
- Limit switches: The crank clutch unit has 12 single pole double throw limit switches. Six nor-

mally open contacts of six independent switches will close simultaneously to signal engaged clutch position and another group of six switches will signal disengaged clutch position. Five "engaged" and five "disengaged" limit switches out of each group of six switches will be used to meet two-failure tolerant crank clutch position signal criteria. One engaged and one disengaged switch will be used for instrumentation.

QUALITY ASSURANCE PROVISIONS

Verification of the requirements is accomplished by one or a combination of the following methods: analysis, similarity, test, and inspection. The test program associated with the DA rotation is shown in Table 1 and summarized as follows.

- Individual Acceptance Tests (Hoover Electric Company)
- Qualification Tests (Hoover Electric Company)
- Design Evaluation Tests (General Dynamics)
- Factory Acceptance Tests (General Dynamics)
- Eastern Launch Site (ELS) Ground Checkout Tests (NASA/General Dynamics)

The purpose of this extensive test program is to demonstrate adequacy of the design for the intended use and support two-failure tolerant capability. Qualification test durations are four times the duration of the anticipated number of mission duty cycles. Qualification testing will begin in August 1984 in parallel with the Design Evaluation Test.

TWO-FAILURE TOLERANCE RATIONALE

Interpretation of redundancy, associated with static and dynamic component design, serves to determine two-failure tolerant characteristics.

There are inherent problems in the practical application of a two-failure tolerant electromechanical system that can be effectively studied in parallel with manned Orbiter missions. With the presently available technology and many different interpretations of redundancy, it is extremely difficult to design a truly two-failure tolerant transmission arrangement that transmits motive force from the electric motor to the link by gears, through a crank, while the crank is engaged by a clutch. This arrangement must also be simple, lightweight, inexpensive, and most of all reliable.

Employing multiple levels of redundancy in electrical or fluid power transmission is relatively trouble free. Electricity or fluid media can be switched readily to maintain a continuous power supply, and a jammed relay or valve does not hinder the course of action. Jamming of a mechanism, however, can stop an operation which can lead to hazardous situations.

A two-failure tolerant electromechanical design becomes complicated, especially in cases where more than one component can jam. Jam removal capability must be provided to allow continuation of the function in case the primary system stops functioning (first failure) and switching to the backup system is impossible for any reason (second failure).

Assume that a two-failure tolerant remotely controlled mechanism has three independent means of accomplishing the assigned task or function. To switch from the first to the second

Table 1
DA Rotator Test Program

Qualification	Acceptance	Design Evaluation (CISS horizontal)	Factory Acceptance (CISS vertical)	Ground Checkout at ELS (CISS horizontal and/or vertical)
Acceptance Humidity Explosive atmosphere Vibration Endurance vibration Pyrotechnic shock Thermal vacuum Thermal cycle Crank oscillation Cycling Mechanical limits Stiffness Motor Bonding EMC Electrical stress Performance Post test disassembly & examination	Examination of product Performance Functional Vibration Thermal cycle Power consumption Cycling Performance	DA rotation Primary & backup modes verification Electrical parameters Landing loads Rotational spring rates Torque limiter External failure modes Clearances	Counterweight installation/removal verification DA rotation Primary & backup modes verification Electrical parameters Torque requirements Clearance verification	DA rotation Primary & backup modes verification Electrical parameters Power requirements verification DA 0 and 45 degree position verification Visual clutch position indication verification

means and from the second to the third means, remotely controlled jam removal methods are required for the engaging/disengaging mechanism of the first and second means. The combination of the first and second jam removal methods must be two-failure tolerant. If pin pullers are used for jam removal, link capturing devices must be provided for the first and second means. The combination of the first and second link capturing devices must be two-failure tolerant. This system is complicated, heavy, expensive, and requires complex avionic and software systems. Reliability may be degraded because of the complexity.

Ideally, there should be only one super-reliable means of performing the function, with a sufficient degree of built-in redundancy. If external jamming of the system is credible, a backup means is required and the primary means must be provided with redundant jam removal capability to allow the backup to function.

The DA rotation system design follows the definitions, ground rules, and reliability techniques of Reliability Desk Instruction DI No. 100-2F, Failure Mode Effect Analysis (FMEA), established for the Space Shuttle Orbiter subsystems to verify design adequacy with respect to inherent reliability. Some definitions and ground rules from this document follow.

Definitions

- Failure — Inability of a system, subsystem, component, or part to perform its required function within specified limits under specified conditions for a specified duration.
- Failure Mode — A description of the manner in which an item can fail.
- Hazard — The presence of a potential risk situation caused by an unsafe act or condition.
- Redundancy (depth of) — The available (number of) ways of performing a function*.

  *NASA SP-7, Dictionary of Technical Terms for Aerospace Use, defines redundancy as "the existence of more than one means for accomplishing a given task, where all means must fail before there is an overall failure to the system."

  "*Parallel redundancy* applies to systems where both means are working at the same time to accomplish the task, and either of the systems is capable of handling the job itself in case of failure of the other system. *Standby redundancy* applies to a system where there is an alternative means of accomplishing the task that is switched in by a malfunction sensing device when the primary system fails."

  Per Webster, the definition is "more than enough" or "superfluous." This interpretation may be the key to achieving equivalent safety by overdesigning the appropriate mechanical components instead of reaching for alternate means.
- Backup Mode of Operation — The available way(s) of performing a function using "like" (identical) hardware.
- Alternate Mode of Operation — Any additional ways of performing a function using "unlike" hardware.
- Criticality — The categorization of a hardware item by the worst-case potential direct effect of failure of that item. In assigning hardware criticality, the availability of redundancy is considered. Assignment of functional criticality, however, assumes the loss of all redundant (backup or alternate) hardware elements.
- Single Failure Point — A single item of hardware, the failure of which would lead directly to loss

*NASA SP-7, Dictionary of Technical Terms for Aerospace Use—Definition of redundancy

of life, vehicle, or mission. Where safety considerations dictate that abort be initiated when a redundant item fails, that item is also considered a single failure point.

- Critical Item – A single failure point or a redundant element in a life or mission-essential application where:
  a. Redundant elements are not capable of checkout during the normal ground turnaround sequence.
  b. Loss of a redundant element is not readily detectable in flight.
  c. All redundant elements can be lost by a single credible cause or event such as contamination or explosion.

Ground Rules

- Dual redundancy:
  a. The first failure would result in loss of mission.
  b. The next related failure would result in loss of life or vehicle.
- The loss of all redundant elements by a single credible cause or event is considered unlikely.
- Where redundancy exists in the subsystem, the redundancy is considered during failure analysis.
- "Alternate means of operation" refers to accomplishment of a function and not necessarily to redundancy or restoration of a failed function.
- Failure of structural items (primary or secondary) will not be considered in this analysis. (Structural items are assumed to be designed to preclude failure by use of adequate design safety factors.)

The FMEA for the rotator has been prepared and submitted by Hoover Electric as part of the vendor critical design review.

WAIVER

A waiver request was submitted to the customer specifically to exclude clutches and gear trains inside sealed gear boxes, as well as linkages from multiple level redundancy requirements. This approach is similar to the rationale employed in the Orbiter electromechanical technology, waiving gearing, linkage, and structural component failures as being unlikely (noncredible).

There are indications, however, that this waiver may not be approved for the full-length payloads, which block LVA egress. Suggested solutions are:

a. Addition of a remotely actuated pin puller and capture device to the primary rotator link. This would allow the primary rotator link to be "broken" if the primary drive and clutch disengagement mechanisms both failed. Rotation could continue using the secondary rotator system.

b. Use of an energy storage device (e.g., a spring) to hold the stack in a normally-stowed position with remote pin-pullers at the drive links in case of multiple mechanism failure. Actuation of the pin pullers would result in automatic return of Centaur/payload stack to its stowed configuration.

c. Design of the clutches so that if the primary clutch fails to disengage, the backup rotator

can produce sufficient torque to cause the primary rotator clutch to slip, thus permitting rotation to continue.

Other suitable methods may be studied to develop acceptable design modifications to meet the two-failure tolerance requirement or achieve equivalent safety. In view of the criticality of the G-prime schedule, it would be impractical to impose any unique payload requirements on the G-prime rotation system at this time.

RATIONALE FOR ACCEPTANCE

Summary — Two-failure tolerance is provided to the maximum extent practical. Two independent rotator systems are provided. Each system includes a power drive unit that contains two independent drive motors. Each of the two motors in each power drive unit is capable of rotating the Centaur up for launch (separation) and down to stow for landing. Each power drive unit engages its rotation linkage through a clutch that is actuated by one of two independent motors. Such engagement does not occur until just before rotation in orbit. Three independent ac power sources are switched through the two-failure tolerant avionics system to provide two-failure tolerant power to each power drive and clutch motor. Each motor is controlled by an ac source, in which three independent series inhibits are placed. If any two ac sources, inhibits, or control units fail, the system will not rotate inadvertently and will still permit up or down rotation. The system meets the two-failure requirements in all components except the power drive unit clutches, geartrains, and structural linkage. An engaged clutch that fails to disengage, in conjunction with a jammed geartrain in the same power drive unit, would prevent rotation of the Centaur, as would failure of both clutches or geartrains. However, the combination of the drive and clutch motors of the primary and backup rotators are quad redundant, while each rotator is responding to triple redundant avionic command inputs. It should be noted that the DA rotation system has a higher level of failure tolerance than any Orbiter electromechanical system. For instance, any of the three active payload holddown latches jammed in the latched position will prevent rotation of the Centaur and block EVA.

Discussion — The sequence used to rotate the Centaur after the cargo bay doors are opened is as follows:

- The Orbiter turns on ac1 and ac2 (ac3 is always present at the Orbiter interface).
- Commands from the standard switch panel (SSP) will start Centaur airborne support equipment (CASE) controlled operations by engaging the primary clutch with motor 1. If this motor fails, motor 2 will automatically be activated. When the clutch is fully engaged, the motor (1 or 2) is turned off.
- The Orbiter commands the release of its Centaur holddown latches.
- Commands from the SSP will then activate the primary drive motor 1 and automatically rotate the Centaur out of the cargo bay. If this motor fails, primary drive motor 2 will automatically be activated to rotate the Centaur.
- At the erected position, the drive motor (1 or 2) is turned off automatically. The Orbiter may then secure power sources ac 1 and ac 2.

If a failure(s) occurs that prevents or halts Centaur rotation, the CASE control system will automatically switch over to the completely separate and redundant backup rotator system. Rota-

tion may then be continued by reinitiating commands from the SSP to erect or stow the Centaur. The CASE control system will then activate the components of the backup system in the same manner and sequence as previously mentioned to continue engagement or rotation.

The Orbiter crew can use the SSP to override or back out of the primary or backup operational sequence at any point. This includes returning the Centaur to the completely stowed position for a mission abort.

The DA rotation system is safe as designed and analyzed and may be classified as a cargo element/payload of the Orbiter for the following reasons:

- Each rotator is capable of performing a minimum of 1,000 duty cycles during its operating life, which is far in excess of the 10-mission requirement. The structural ultimate factor of safety is 1.4 (minimum). The components of the system have adequate strength and stiffness. Gear stress levels are one-fourth of the material ultimate stresses.
- Clutches are designed with separation springs between the clutch plates to prevent binding after the clutch is disengaged.
- Bearings, such as those used for the links, incorporate multiple rotating surfaces to ensure that rotational capability exists following surface-to-surface binding of one rotating surface. The life of each rotational surface is adequate to meet the full operating life of the item. If multiple rotational surfaces are not provided, the L10 life of each bearing or rolling element will exceed the required life by a minimum factor of 17.
- In case multiple sliding surfaces are not provided, the normally lubricated surfaces will slide without lubrication, thus providing one-failure tolerance. Also, test and design data obtained from the manufacturer show that the minimum power available to restow the Centaur is 3.2 times the worst-case restow forces.
- To prevent a single-point structural failure, the single structural component and the clutch components have built-in redundancy by oversizing the component for strength. In this case, the limit load is modified to include a suitable safety factor, and the maximum anticipated load is multiplied by that chosen safety factor. Selection of the redundancy safety factor depends on individual credible failure modes related to the function of the single component and analyzed on a case-by-case basis.
- The crank remains in its last actuated position until powered to a new position. Neither an out-of-tolerance condition nor a single component failure affects holding of position or moving to a new position.
- Threaded parts and fasteners are positively locked to prevent loosening during service. Single-fastener attachments have dual-locking features.
- Gearboxes are designed to preclude entry of foreign materials, loss of lubricants, and jamming of gears. No threaded fasteners are used inside the gearbox. Internal volume is kept to a practical minimum.
- Qualification tests will be performed to prove functional capability under extreme environmental conditions. Ground checkout tests before launch and ELS quality control operations will be performed.
- The manufacturer, Hoover Electric, has demonstrated the capability for designing and building similar devices, as exhibited by various electromechanical actuators provided for the Space

Shuttle vehicle (e.g., external tank umbilical door drive actuator, external tank umbilical door centerline latch actuator, external tank umbilical door latch drive actuator, payload bay door bulkhead latch actuator, payload bay door centerline latch actuator, radiator panel latch actuator, radiator panel drive actuator, and manipulator positioning mechanism actuator). The DA rotator employs the same concepts and some identical hardware used in these flight-qualified actuators.

CONCLUSION

The DA rotator design has required state-of-the-art space technology to produce a very reliable rotation system for the Centaur G-prime and G vehicles. Proper interpretation of redundancy is essential for hardware acceptance. This can be demonstrated by using proven electromechanical design methods, careful selection of materials, and with full understanding of hardware and functional criticalities. Simplicity and commonality can greatly improve reliability and safety while achieving mission objectives. Interpretation of redundancy is necessary to facilitate the method of attaining equivalent safety that matches the effect of two-failure tolerance by overdesigning the single critical components. Gears, clutches, and linkage are not two-failure tolerant; however, they are considered acceptable because of ultra-conservative wear, stress, and life factors. The author's observation is that a more explicit definition and guidance tailored for electromechanical designs for space application would be instrumental in equating redundancy to equivalent safety based on credible failure modes of individual components and would help eliminate doubt during the design phase. Differing definitions of redundancy can lead to disagreements resulting in possible design changes impacting schedule and cost.