DESIGN OF A DUAL FAULT TOLERANT SPACE SHUTTLE PAYLOAD DEPLOYMENT ACTUATOR

DUANE R. TESKE*

ABSTRACT

As the Shuttle Transportation System (STS) becomes operational, the number and variety of payloads will increase. The need to deploy these cargo elements will require a variety of unique actuator designs, all of which will have to conform with STS safety policy.

For those missions where payload operations extend beyond the payload bay door envelope, this policy deems the prevention of door closure as a catastrophic hazard. As such, it must be controlled by independent, primary and back-up methods. The combination of these methods must be two-fault tolerant.

This paper describes the design of such an actuator. The device consists of a single linear ballscrew with two ballnuts, each ballnut forming an independent actuator using the common ballscrew. The design requirements, concept development, hardware configuration, and fault tolerance rationale are highlighted.

INTRODUCTION

An Orbiter based satellite delivery system is presently under development. Comprising an upper stage and associated airborne support structure, this system is carried "lying down" within the Orbiter bay and raised from the bay for deployment, Figure 1. As the raised element extends beyond the payload bay door envelope, failure could impede door closure and prevent safe return of the Orbiter. The actuator system thus can cause a catastrophic hazard, requiring control by independent primary and backup methods, the combination of which must be two-failure tolerant.[1]

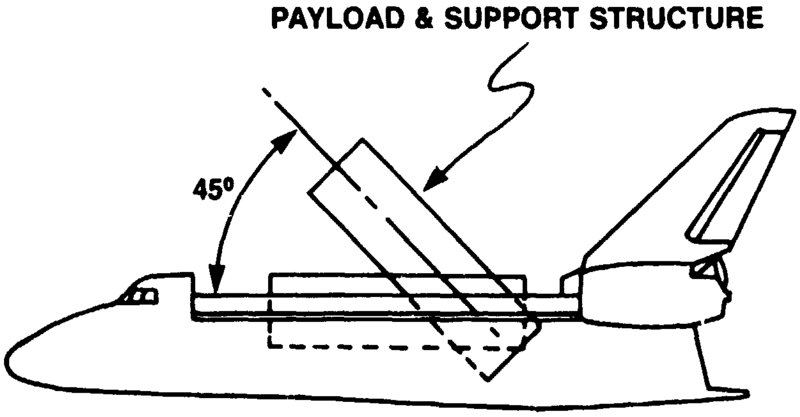


Figure 1 Payload Deployment Schematic

*Sundstrand Energy Systems, Rockford, Illinois

CONCEPT DEVELOPMENT

A survey of existing deployment systems was made to determine if any were adaptable to this application. In general, dual fault tolerant capability is achieved by using two actuators.

The shortcoming of this approach, however, is the ability of a failed actuator to lock the entire drive train, defeating the backup unit. Either extra vehicular activity (EVA) or a disconnect mechanism, such as a pyrotechnic device,pin puller or clutch is, therefore, required. However, each device adds its reliability factor to the system and increases complexity. In addition, to prevent inadvertent disconnection of the healthy unit, either a method of discriminating the failed actuator must be devised,or a mechanism which allows reliable reconnection must be conceived. Similarly, a retention/stowage device for the disconnected unit is often required.

Existing systems solve this problem in various ways, but with considerable proliferation of parts. Further, such solutions usually result in a number of items or functions which cannot be allowed to fail. These "noncredible" failure items are always the subject of debate and generally increase the precision of manufacture required.

Nevertheless, in an attempt to improve existing designs, several dual actuator design studies were made. All the resulting concepts, however, offered only marginal improvement. As a result, a single actuator system which would possess the necessary fault tolerance was sought.

DESIGN DESCRIPTION

The single actuator design concept which evolved is illustrated in Figure 2. The mechanism consists of a linear ballscrew upon which are mounted two independent ballnuts. Each ballnut is enclosed in its own housing, forming, in essence, an independent actuator free to transit a portion of the ballscrew. The mounting arrangement of the actuator, Figure 3, is such that retracting the actuator raises the payload and extending the actuator lowers it.

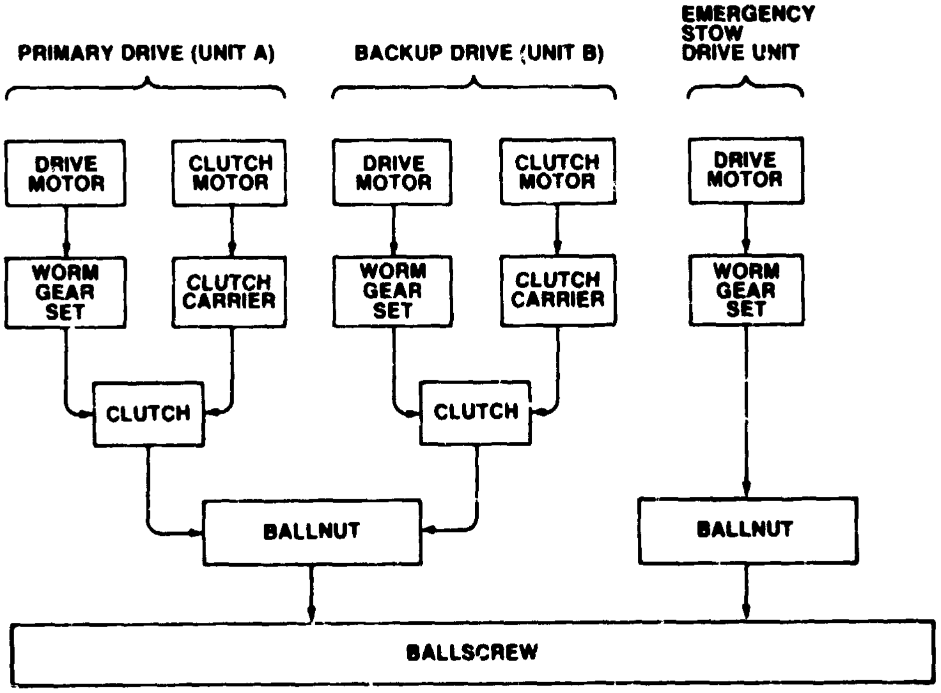


Figure 2 Actuator Block Diagram

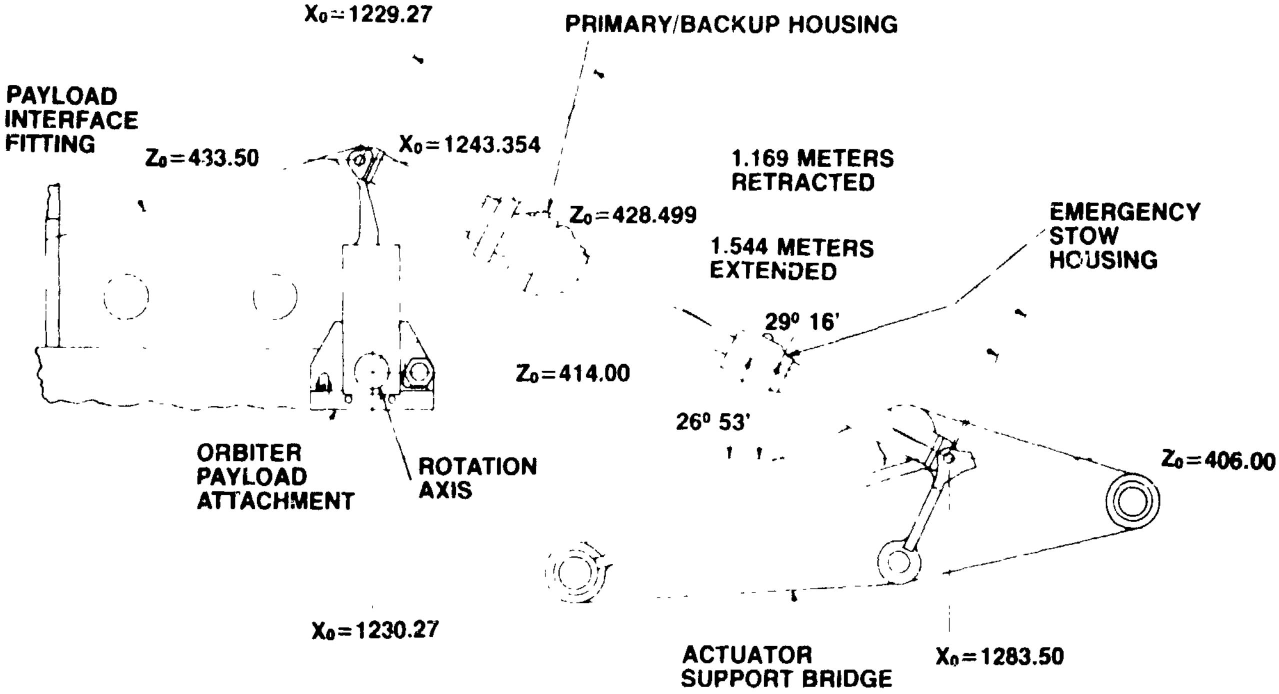


Figure 3 Actuator Installation

Dual-fault tolerance is achieved by providing each actuator half with the full stroke necessary for the application. For normal operation, one ballnut is used to extend or retract the actuator, Figure 4. Two independent methods of driving this ballnut are provided, permitting full mission performance even with one failure.

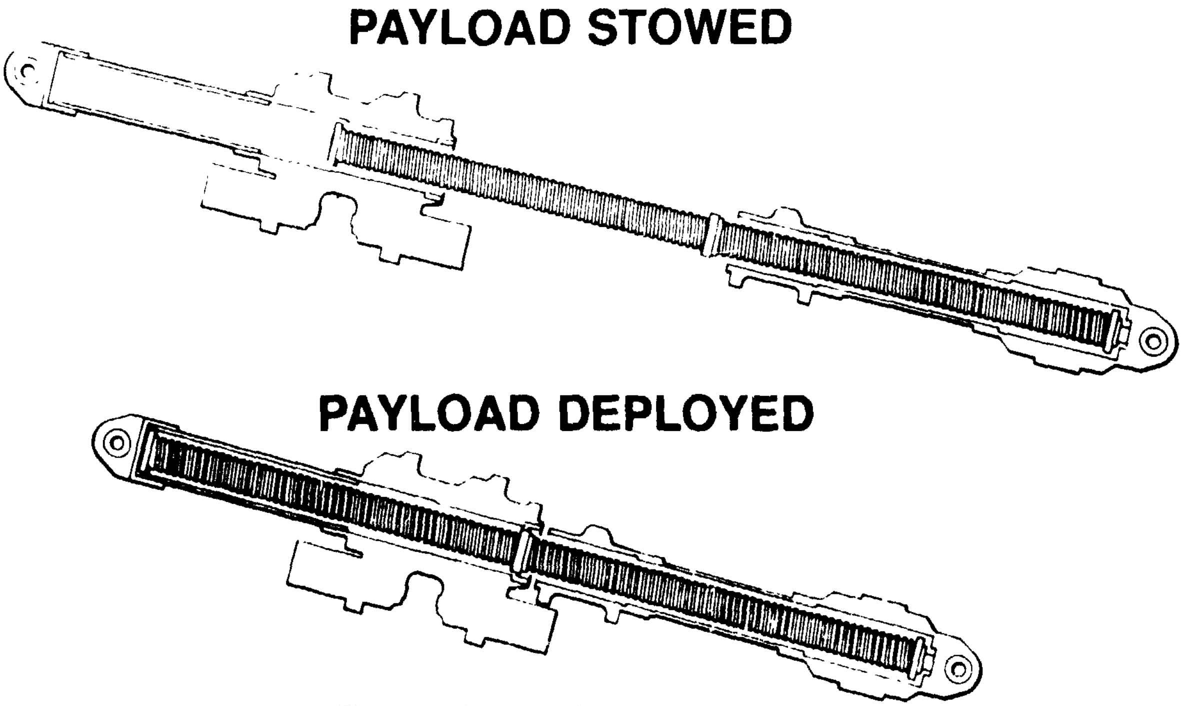
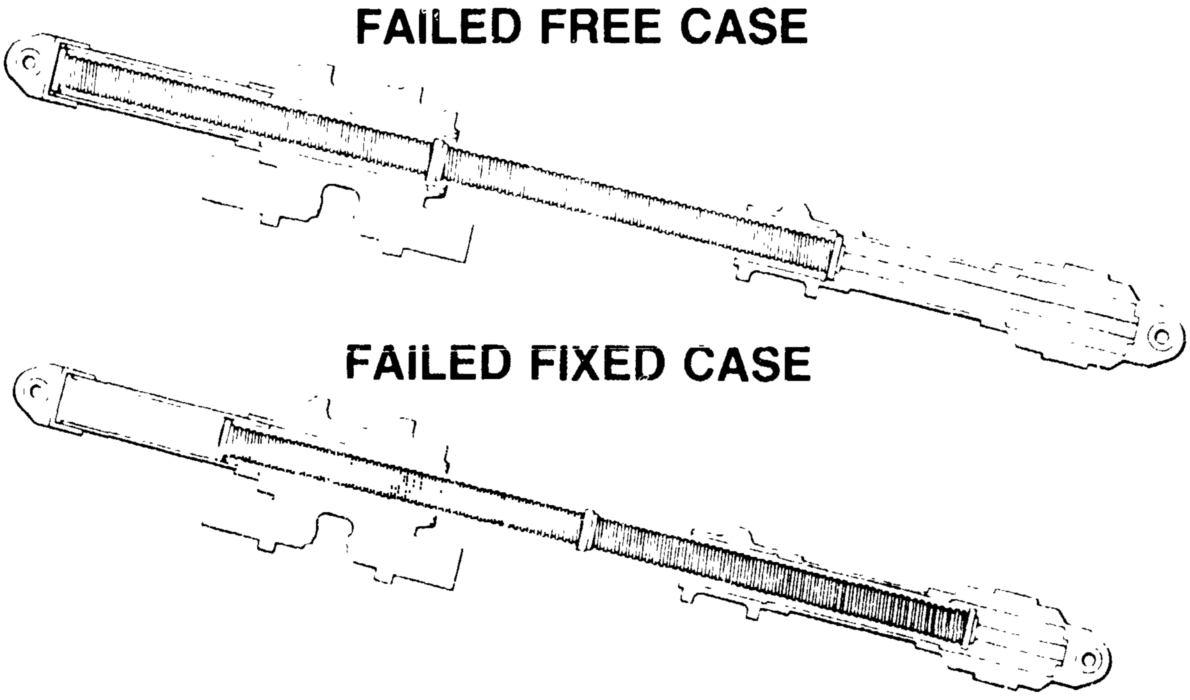


Figure 4 Normal Operating Sequence

If a combination of two failures immobilizes this primary and backup system, the second ballnut is activated. This portion of the actuator serves as an emergency stowing unit by paying out the additional stroke length which is stored within its housing Combinations of failures which have resulted in either failed fixed or failed free situations in the primary backup unit can be handled equally, Figure 5. The emergency unit is also geared higher than the primary backup to provide additional force capability in emergency situations. This arrangement thus possesses single fault tolerance with respect to fulfilling mission performance and dual fault tolerance in controlling the catastrophic hazard.


FAILED FREE CASE

FAILED FIXED CASE

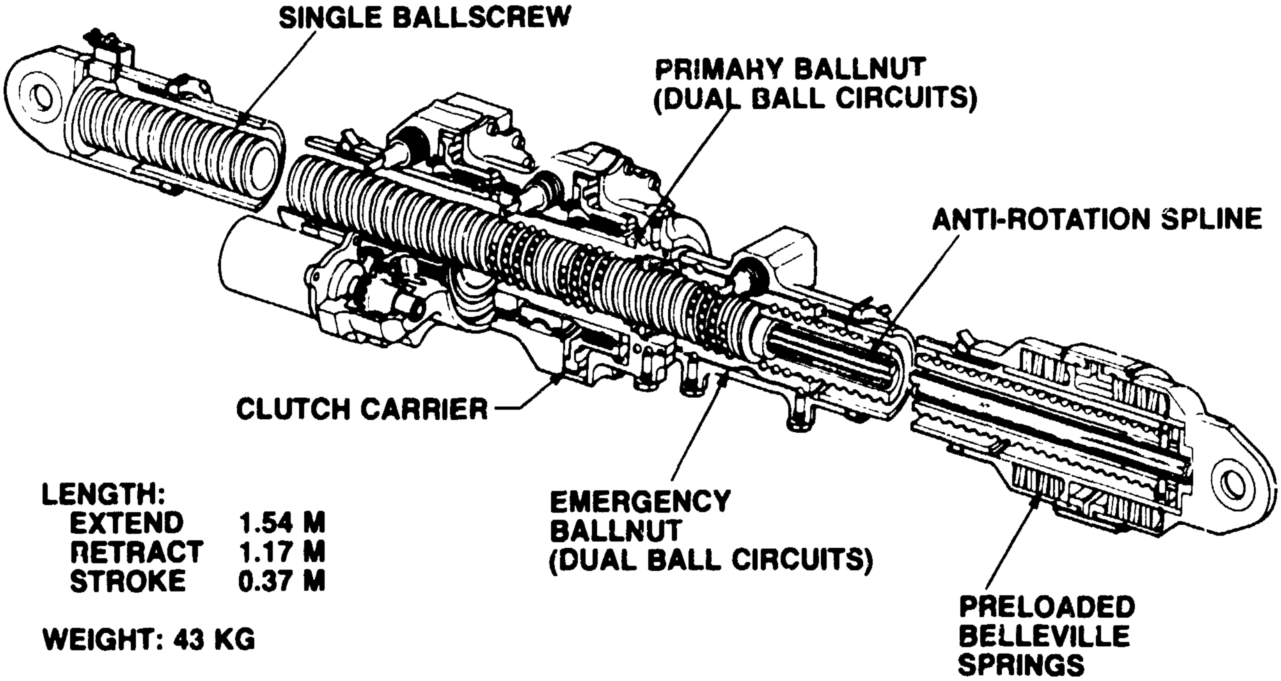
Figure 5 Emergency Stow Operation

In addition, the number of single point failure items which need "noncredible" status has been greatly reduced. Most are controlled in a straightforward fashion. Single load path items, using methodology similar to that for the vehicle structure, are designed for generous safety margins and subjected to fracture analysis and control. Critical rotating interfaces are provided with two independent rotating surfaces. Single fastener attachments have two independent methods of retention.

Inspection of the block diagram in Figure 2, however, will reveal that jamming of both ballnuts (two failures) will render the mechanism inoperative, defeating the two fault tolerant philosophy. Design features employed to render this a noncredible failure mode include two independent ball circuits in each nut; fits, finishes, lubrication, and materials which provide a calculated life well above the intended use; non-jamming wipers on ballnut external interfaces, plus adherence to a contamination control plan for manufacture, assembly, and test. Small parts internal to the actuator's housings are also retained or captured to prevent their loosening and migrating to the ballnut interface. Based on over 21,000,000 hours of operation on similar Sundstrand ballscrew actuators, these controls permit a ballnut/ballscrew assembly to be considered an intrinsic single-failure tolerant device.

ORIGINAL PAGE IS
OF POOR QUALITY

The resulting actuator is illustrated in Figure 6. Actual weight of an engineering prototype is 15% less than that calculated for a comparable dual actuator system.


SINGLE BALLSCREW
PRIMARY BALLNUT (DUAL BALL CIRCUITS)
ANTI-ROTATION SPLINE
CLUTCH CARRIER
EMERGENCY BALLNUT (DUAL BALL CIRCUITS)
PRELOADED BELLEVILLE SPRINGS

LENGTH:
EXTEND 1.54 M
RETRACT 1.17 M
STROKE 0.37 M

WEIGHT: 43 KG

Figure 6 Actuator Cutaway

DESIGN CONSIDERATIONS

In addition to the fault tolerance requirements, other performance issues impose design constraints, many often conflicting, Figure 7. For example, stability in launching the spacecraft is necessary to avoid collision with the airborne support structure. This dictates a low backlash, high stiffness actuator to prevent pitch oscillations as the spacecraft pushes off and exits the cargo bay. High stiffness is also desired to prevent dynamic coupling of the cargo element with the Orbiter thrusters during payload erection and stow.

Safety

- Independent Primary and Backup Actuation Methods
- Combination of Primary and Backup Methods Must Be Two-Failure Tolerant

Operational

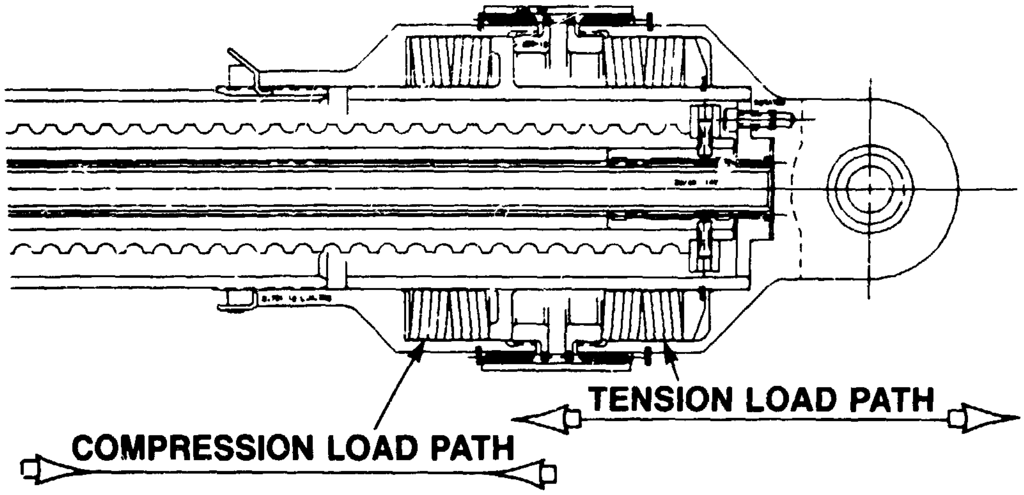
- Erect the Payload to Any Angle From 0° to 45° in Less Than 10 Minutes
- Maintain High Stiffness/Low Backlash to React Upper Stage Separation at Any Angle
- Prevent Backdriving Under Load
- Maintain a Minimum Force Capability of 5340 Newtons Over the Operating Environment
- Provide an Emergency Force Capability of 15,570 Newtons
- Limit the Maximum Force From Combined Impact Loads and Actuator Output to a Level Compatible With Orbiter Structure
- React Orbiter Vernier and Primary Reaction Control Loads
- Minimize Dynamic Coupling Between the Orbiter and the Payload
- Minimize Telemetry and Monitoring Requirements to Permit Minimal Crew Involvement
- Provide 10 Mission Life

Figure 7 Requirements

However, during Orbiter launch and landing, the vehicle will be subjected to structural deflections and vibration environments that cause relative motion between the two actuator mounting points. A stiff actuator in this situation can potentially impart undesirable loads to the supporting structure.

The initial design solution was to accommodate the motion through free-wheeling of the unclutched primary/backup ballnut. However, there was a degree of uncertainty as to the ability of the ballnut to respond rapidly enough to attentuate loads at higher frequencies. In addition, a clutch-engaged failure occurring during deployment can defeat this feature for the subsequent landing.

For these reasons, a load relief device was conceived, Figure 8. Consisting of preloaded bellville springs, the device presents a stiff actuator up to 26,690 newtons (6,000 lb) axial load, either compressive or tensile. Above 26,690 newtons, deflection of the device accommodates the relative motion of the mounts without overloading the structure, Figure 9.



Preload = 26,690 Newtons
Travel = 1.57 MM @ 37,810 Newtons

Figure 8 Load Relief Device

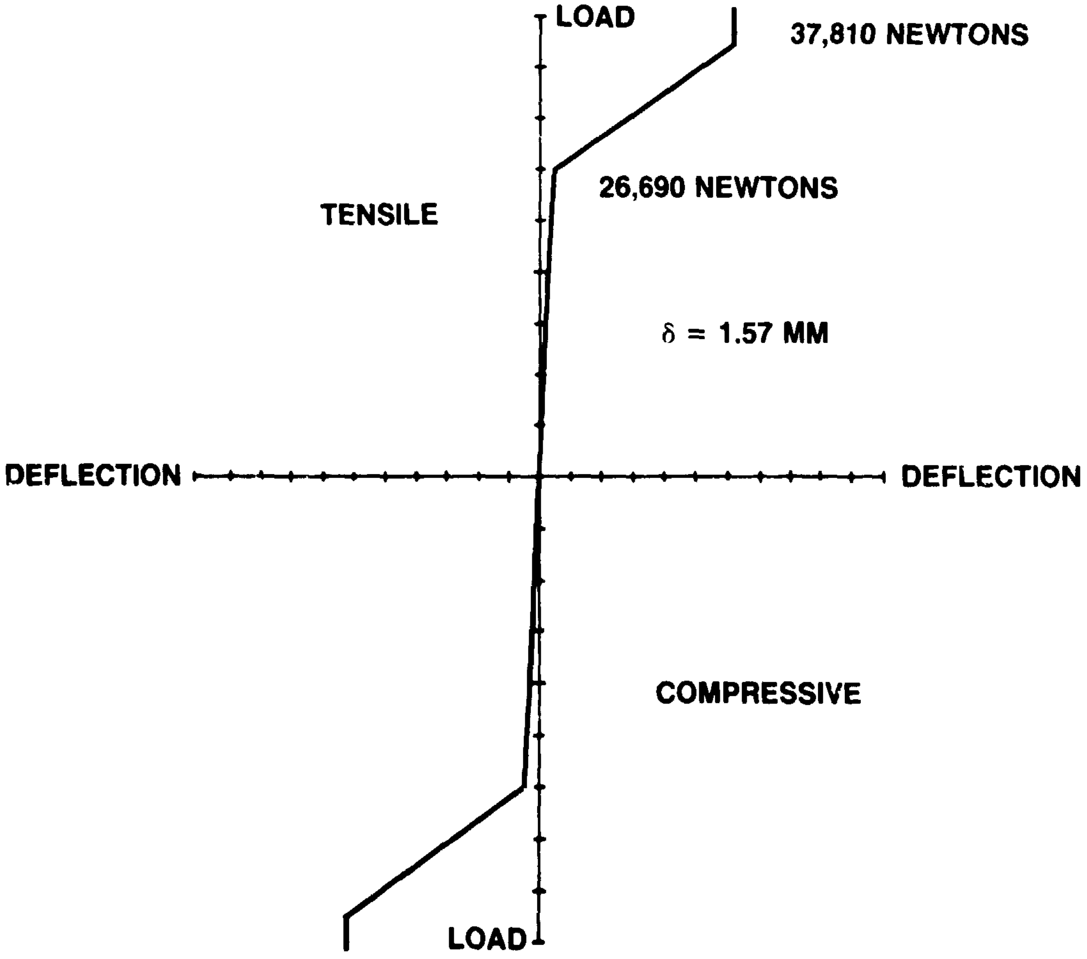


Figure 9 Load Vs. Deflection for Load Relief Device

Fault tolerance considerations extended to the design of the load relief device. Springs were sized such that adequate preload would remain after two spring failures.

The need for load relief is predicated on two factors, the ascent/descent vibration induced deflections and the strength limitations of the mounting structure. Both of these areas incompletely defined at the time the actuator was designed. For that reason, the load relief device was designed to be modular, permitting its easy removal if subsequent tests and analyses should indicate it to be unnecessary.

Competing requirements also arose in establishing the force vs. speed characteristics of the actuator. In service, the actuator can be subjected to a variety of loads as illustrated in Figure 10. Because the dynamics of the interaction between the cargo element and the Orbiter are complex, the precision with which these loads could be defined was uncertain. In addition, the loads are bi-directional, capable of either aiding or opposing actuator motion. Yet the actuator has to provide sufficient force capability to perform at all credible load combinations. Operating force requirements of 0 to 1600 newtons (360 lb), which excursions to 15,520 newtons (3,500 lb), were specified.

- **Operating (On-Orbit)**
  - **— Vernier Reaction Control System**
  - **— Primary Reaction Control System**
  - **— Dynamic**
  - **— Stop Impact at 45°**
  - **— Spacecraft Upper Stage Separation**
- **Nonoperating (Ascent/Descent)**
  - **— Random Vibration**
  - **— Shock**
  - **— Structural Deflections**

Figure 10 In-Service Loads

In providing sufficient force capability to satisfy these requirements, it was necessary, however, to limit the maximum force potential of the actuator so that the mechanism's output would not exceed the strength of surrounding structure. This consideration limited the maximum actuator output to 37,810 newtons (8,500 lb).

In a similar manner, establishing the actuation speed required balancing the desire to deploy in a reasonable time with the maximum insertion speed of the Orbiter's payload retention latch assemblies. The combination of these speed and force requirements served to define an acceptable operating envelope as shown in Figure 11. The actuator design had to satisfy this envelope under all combinations of supply voltages, environments, and manufacturing tolerances.

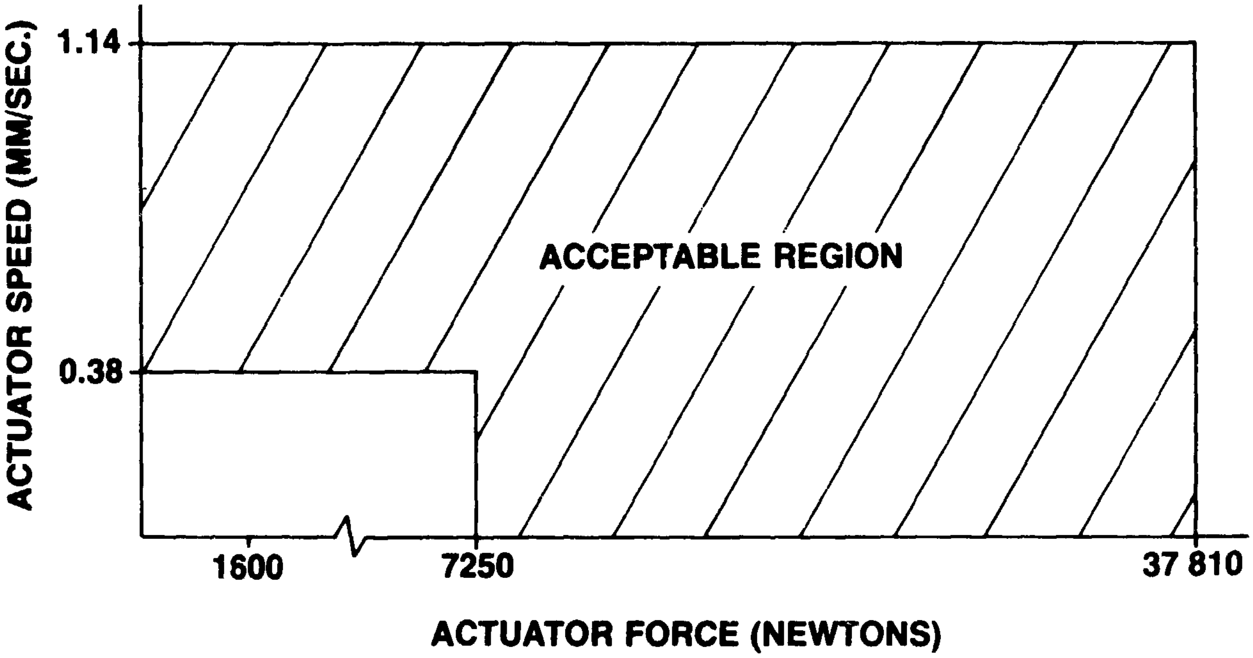


Figure 11 Design Operating Envelope

STATUS AND CONCLUSION

An engineering prototype is presently (November 1984) undergoing performance testing. As noted, this unit is 15% lighter than the calculated weight for the comparable dual actuator system.

More significantly, the actuator design has passed a preliminary NASA Safety Review, a step necessary for acceptance as a Shuttle cargo. This Safety Review has historically resulted in design changes for dual actuator systems.[2] The relative simplicity of the single actuator design and the minimum number of noncredible failure situations facilitated this acceptance.

Although this design has the drawback of requiring the room to accommodate a long mechanism, the approach to fault tolerance is an advantage. It offers a simpler, lighter system with considerable performance versatility.

REFERENCES

1. "Safety Policy and Requirements for Payloads Using the Space Transportation System", NHB 1700.7A, December 1980, P. 2-4.

2. Hornyak, Stephen, "Inherent Problems in Designing Two Fault Tolerant Electromechanical Actuators", *Proceedings 18th Aerospace Mechanism Symposium*, May 1984, NASA Conference Publication 2311.