PREFERRED RELIABILITY PRACTICES

REDUNDANCY IN CRITICAL MECHANICAL SYSTEMS

Practice:

The careful use of redundancy in Critical Kennedy Space Center (KSC) Ground Support Equipment (GSE) Mechanical Systems ensures reliable operation.

Benefits:

The benefit of using dual redundancy in critical KSC GSE systems is greater assurance of successful system operation during critical shuttle processing operations in the event of a single equipment failure that would otherwise possibly cause loss of life, vehicle or damage to a vehicle system. By designing in redundancy for critical operations, the system can fail to a "fail-safe" condition and still achieve operational objectives.

Programs Which Certify Use:

KSC Ground Support Equipment

Center to Contact for More Information:

Kennedy Space Center, Florida

Implementation Method:

The Orbiter Access Arm (OAA) is a critical GSE system located at Launch Complex 39, Pads A and B, Kennedy Space Center, Florida. The OAA is extended shortly after the shuttle arrives at the launch pad to allow personnel access to the shuttle to make the necessary preparations for launch. Shortly before launch, the astronauts will board the shuttle via the OAA. The OAA provides the only path of ingress and egress to the space shuttle crew cabin for the astronauts. Thus, this system becomes critical to the safety of the crew.

A critical system, as it applies to KSC GSE systems, is a system whose loss of overall system function, or improper performance of a system function, could result in loss of life, loss of the shuttle vehicle itself, or damage to a shuttle system. In addition, systems that have been identified as critical must be designed to be fail-safe. Fail-safe design provides the ability to sustain a critical system failure without causing loss of life, loss of the shuttle vehicle, or damage to a shuttle system. This includes the capability to safe the systems and successfully terminate operations, or if required, to continue operations through to completion.

REDUNDANCY IN CRITICAL MECHANICAL SYSTEMS

Therefore, the OAA system must be able to sustain a failure and still be able to perform its function to completion of the operation. In the event of a single system failure, it must fail to a safe condition, meaning a single failure will not result in loss of life, loss of the shuttle, or damage to a shuttle system.

The critical condition is encountered when the OAA is retracted away from the shuttle at T-7:30 minutes in the countdown in preparation for launch. Should an emergency arise, either on board the shuttle or on the launch pad, during the final minutes of the countdown after the OAA is retracted, the OAA will need to be re-extended to allow the astronauts to evacuate the area as quickly as possible. Extension of the OAA is essential to the astronauts safety, as it is the only path available to the crew in the event evacuation of the shuttle is required. The astronauts lives depend on the OAA extending when needed.

The probability of 2 redundant components failing during a critical time period is much less likely than 1 component failing during the same period. In the case of the OAA, 2 completely redundant sets of valves, plumbing, and electrical controls are installed. Based on the classical probability theory, assuming no common cause failures, it can be shown that through using dual redundancy the reliability of a system can be increased 1 or more orders of magnitude. Thus redundant system design provides protection against a single failure causing a hazardous condition resulting in loss of life, destruction of a shuttle or damage to a shuttle system.

Technical Rationale:
Redundancy is defined as multiple ways of performing a function. There are several different types of redundancy used on KSC GSE systems. Depending on the requirements of the application, the type of redundancy to be used will vary. The two primary types of redundancy are described below:

- Operational or Active "fully on" Redundancy - Redundant elements, all of which are fully energized during the system operating cycle. Operational redundancy includes load sharing redundancy wherein redundant elements are connected in such a manner that, on failure of one unit, the remaining redundant elements will continue to perform the system function. Switching out the failed element is not required. Operational redundancy may be either full parallel or "majority vote".

- Standby Redundancy - A redundant hardware item(s) that are non-operative until they are switched into the system on failure of the primary item(s). Switching can be accomplished by either automatic or manual means.

Other categorization of redundancy include:

- Like Redundancy - Identical hardware items performing the same function.

- Unlike Redundancy - Nonidentical hardware items performing the same function. Safety features which provide protection for specific failure modes are considered as unlike redundancy for that failure mode; i.e. relief valves which provide protection against overpressurization after failure of a regulator.

Typically, KSC employes parallel, two component redundancy. It can be shown that the incremental reliability gain is greatest for the first redundant unit and decreases rapidly as more redundant units are added in paralle.

Figure 1 provides an example of a basic block diagram of the hydraulic extend circuit for the Orbiter Access Arm (OAA) showing the use of redundancy in a critical shuttle ground support system.

A hydraulic reservoir fills 4 hydraulic accumulators. Only 2 accumulators are needed to ensure arm retract and extend, but 2 additional (redundant) accumulators are provided for fail-safe

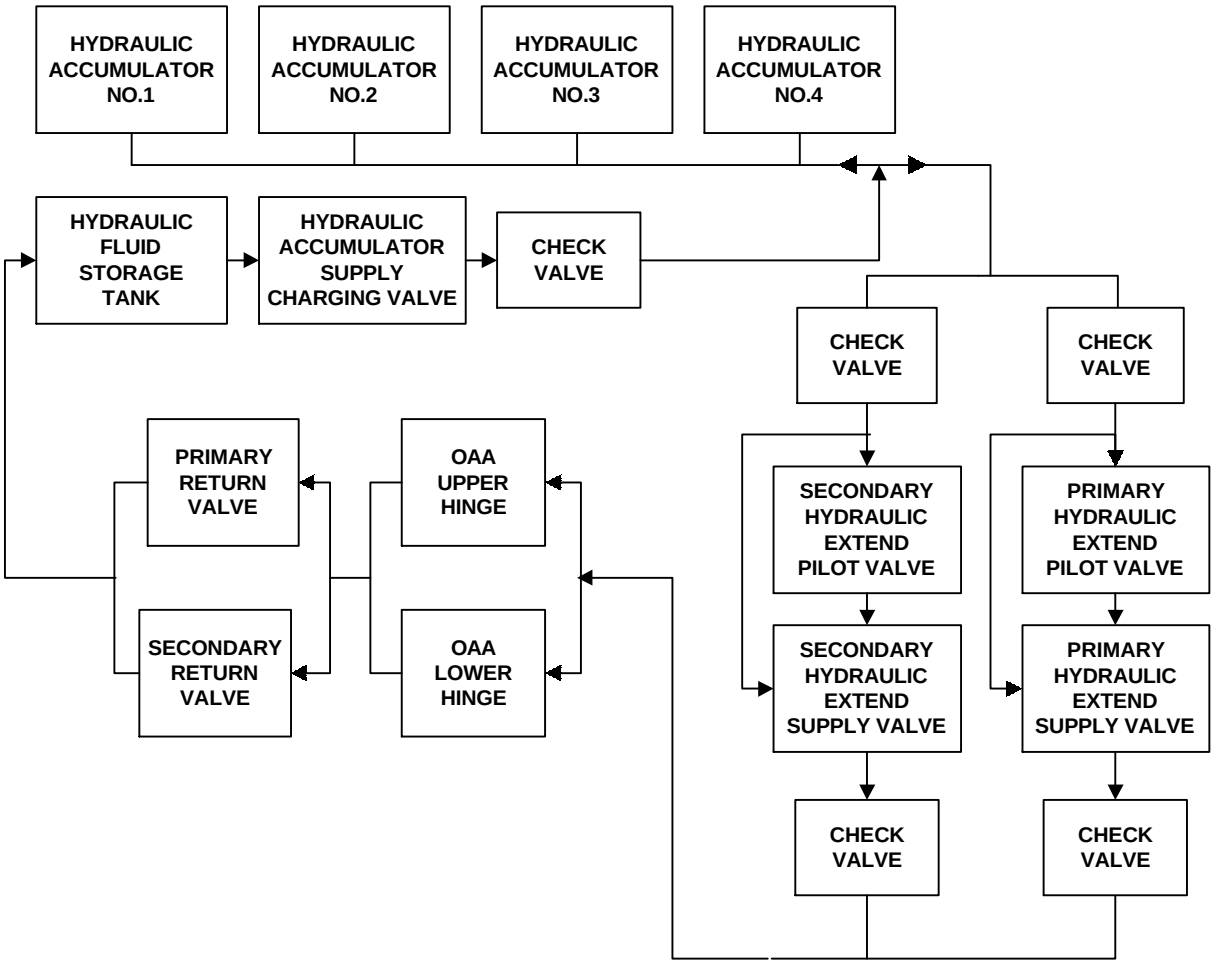

Figure 1 Simplified Block Diagram, OAA Hydraulic Extend Circuit

operation in the event of a leak. In the event of a major leak, the launch countdown will stop. If a major leak occurs during an emergency re-extend operation, the 2 redundant accumulators should supply enough hydraulic pressure to ensure full extension of the OAA. In addition, the hydraulic supply system is capable of supplying additional pressure if required.

The ensuing discussion will address the primary system only. Design of the system minimizes the likelihood of a common cause failure. The accumulators provide hydraulic fluid to a pilot valve (Primary Hydraulic Extend Pilot Valve) and to the main hydraulic supply valve (Primary Hydraulic Extend Supply Valve). When commanded by LPS (Launch Processing System), the pilot valve supplies hydraulic pressure to the Primary Hydraulic Extend Supply Valve and to the Primary Hydraulic Extend Return Valve, thus opening both valves. Hydraulic fluid from the accumulators then flows thru the Primary Hydraulic Extend Supply Valve to the upper and lower OAA hinges. Each hinge is individually capable of rotating the OAA. Thus the hinges are redundant. Fluid exits the OAA hinges, and returns to the main hydraulic reservoir through the Primary Hydraulic Extend Return Valve.

This discussion described the basic operation of the primary hydraulic extend circuit for the OAA. There is a secondary (redundant) set of valves as described above installed in parallel with the primary valves, that simultaneously operate.

Operational redundancy ensures that the OAA will operate when needed. A single failure will not result in a catastrophic consequence.

Impact of Nonpractice:

All other factors being equal, the elimination of redundancy in the system described in this practice would result in a considerably higher probability of failure, the identification of additional critical items and increased probability of loss of life.

References:

O'Connor, Patrick "Practical Reliability Engineering" 2nd Edition, Wiley, 1985