Desigining an Alternate Mission Operations Control Room

Patty Montgomery[1]
NASA, Marshall Space Flight Center, Huntsville, AL 35812, USA

A. Scott Reeves[2]
COLSA Corporation, Huntsville, AL 35812, USA

The Huntsville Operations Support Center (HOSC) is a multi-project facility that is responsible for 24x7 real-time International Space Station (ISS) payload operations management, integration, and control and has the capability to support small satellite projects and will provide real-time support for SLS launches. The HOSC is a service-oriented/highly available operations center for ISS payloads—directly supporting science teams across the world responsible for the payloads. The HOSC is required to endure an annual 2-day power outage event for facility preventive maintenance and safety inspection of the core electro-mechanical systems. While complete system shut-downs are against the grain of a highly available sub-system, the entire facility must be powered down for a weekend for environmental and safety purposes. The consequence of this ground system outage is far reaching: any science performed on ISS during this outage weekend is lost. Engineering efforts were focused to maximize the ISS investment by engineering a suitable solution capable of continuing HOSC services while supporting safety requirements. The HOSC Power Outage Contingency (HPOC) System is a physically diversified compliment of systems capable of providing identified real-time services for the duration of a planned power outage condition from an alternate control room. HPOC was designed to maintain ISS payload operations for approximately three continuous days during planned HOSC power outages and support a local Payload Operations Team, International Partners, as well as remote users from the alternate control room located in another building.

I. Introduction

The Huntsville Operations Support Center (HOSC) is a multi-project facility responsible for 24x7 real-time International Space Station (ISS) payload operations management, integration, and control. Though it was designed for continuous operations, the aging facility was required to power-down for the duration of a weekend to allow Facilities maintenance personnel unrestricted and safe access to perform the required preventative maintenance activities on the building's power and cooling infrastructure. During this weekend, on-board ISS Science would stop as the ground system's infrastructure was powered down.

A solution was sought to preserve services as a short-term goal, while maintaining the flexibility to augment the ability and eventually support a disaster recovery environment. The HOSC Power Outage Contingency (HPOC) was developed as a proof of concept solution intended to provide limited services to International Partners during the maintenance weekends. Through the availability of additional funding, HPOC was quickly expanded to include capabilities to support the local flight team as well as remote users with limited services. HPOC provided effective services during numerous activities, and ultimately supported frequent outages in a single year while the HOSC electro-mechanical systems were overhauled to achieve a physical Tier III[1] status.

As a result of the electro-mechanical upgrades, the HOSC facility is now capable of supporting simultaneous facility maintenance and flight operations. This achievement has left HPOC available for conversion to an Alternate Mission Operations Control Room to provide if needed Disaster Recovery (DR) services for HOSC Operations.

II. HPOC Design

The HPOC is a physically diversified group of systems capable of providing identified real-time services for the duration of a planned power outage from a consolidated computer/mini-control room located in MSFC

[1] Computer Engineer, MSFC/MOL, MSFC/EO50, non-AIAA Member
[2] Senior Systems Engineer, MSFC/MOL, non-AIAA Member.

Building 4207 Annex. The HPOC was designed to maintain ISS payload operations for approximately three continuous days during planned HOSC power outages. HPOC Core Systems reside in portable rack assemblies. These racks are organized in a compliment of five rack enclosures – four racks located in the HPOC facility and one rack located in Building 4663, A109D

Many short and long term goals were considered when designing HPOC. These were evaluated thoroughly to ensure the success and maximized potential of HPOC over time. The HPOC architecture was established to pursue the short term goals while supporting a long range plan that has been achieved since the HOSC Facility Improvements.

The short term goal of HPOC was to provide specific services to specific customers during planned HOSC facility power outages. The initial scope of support included only real-time Ku-Band Telemetry Data Distribution and Archiving for International Partners. The intent was to ease the task of scheduling HOSC facility outages by decreasing the impact for the international community. Some HOSC International Partners have a gateway presence. These include Japan Aerospace Exploration Agency (JAXA), European Space Agency (ESA), and Agenzia Spaziale Italiana (ASI). The support scope broadened to include remote users, and an evolving Alpha-Magnetic Spectrometer (AMS)[2] payload ground system.

Along with this customer-base and basic delivery, the basic distribution requirements expanded into a comprehensive suite of services:

- Ku-Band telemetry processing and distribution to International Partners.
- Mission Voice Services with a maximum of (96) external real-time Mission Voice loops provided when the HPOC system is operational (Four T-1s, with external dependencies). While HPOC is operational, Mission Voice is made available to the HOSC IST to allow collaboration with International Partners
- Database Services.
- S-Band and Ku-Band Telemetry Processing. Ku-Band data is processed and stored by the HPOC system (48-Hour capacity limitation) during Acquisition of Signal (AOS) periods.
- Temporary Data Archival. The Ku-Band data stored by the HPOC system is merged with the HOSC Archive following the HOSC power outage.
- Near Real Time Data (NRT) Services for Remote Users
- Payload Command Services (via Johnson Space Flight Center (JSC) is the normal connectivity)
- Display Services, including S-Band Application Process Identifier (APID) 1000
- System Monitor and Control (SMAC)
- Payload Information Management System (PIMS)
- ISS Streaming Video Display
- Log Tools
- Limited Planning Services (CPS)

The long-term goal of HPOC was to provide a "Warm" site. An HPOC "warm" site would contain the data links and pre-configured equipment necessary to rapidly start operations, but would not contain live data. Given the frequency of use, it was desired to be able to use the HPOC as a "hot" environment, which mirrored the HOSC in real time. To satisfy the operational need of frequently planned support, it was desirable to enact HPOC Services transparently in real-time from the user perspective. This method is attractive for planned outages of a primary site, but conflicts with the concepts embraced by a fully developed DR capability where services are spontaneously lost while the disaster recovery safeguard is engaged and integrity of data is assessed prior to enablement.

III. HPOC Architecture

The HPOC Systems are modeled to match the Payload Operations and Integration Center (POIC) Systems Architecture. When it is not operationally activated, HPOC interfaces with the HOSC network as an extension of the HOSC operational network. This allows the HPOC environment to be maintained in parallel with existing HOSC hardware and software configurations. All required Virtual Local Area Networks (VLANs) from both the internal and external routers are extended to the HPOC environment's network compliment. The primary difference between the HOSC Systems Architecture and HPOC; as a contingency environment, HPOC is not required to maintain high degrees of availability

HPOC interfaces with the active HOSC Storage Area Network (SAN) for normal operations. HPOC infrastructure also acts with HOSC infrastructure to maintain snapshots of Database storage, Near Real Time (NRT) Data Stores, as well as File Server Resource drives to efficiently maintain an off-site SAN content backup with rollback capability.

The HPOC Network is an extension of the HOSC inner and outer VLAN Trunk Protocol (VTP) domains. Tertiary nodes are employed using proven protocols such as Cisco's High Speed Router Protocol (HSRP). The network was designed to allow for commonality in parallel management, while minimizing the burden of transition to HPOC. The HPOC Network infrastructure consists of the following elements capable of operating independently of the HOSC:

- (Tertiary) Inner Core Router
- (Tertiary) Payload Distribution Data (PDD) Firewall
- (Tertiary) Outer Core Router
- (Tertiary) HOSC & PDD Firewall
- Enhance HOSC Personal Computer Workstation Switch
- Network Sniffer
- Global Positioning System (GPS) Receiver/Time Server
- S-Band Gateway

Transitions to and from HPOC operations involves as little physical intervention as practical. Transition to HPOC is scheduled during Loss of Signal (LOS). The transition to HPOC is transparent to remote users, although this transition is coordinated and data flows are verified.

During activation, HPOC functional resources are limited as-built to support a maximum support staff of:

- Payload Operations Integration Team (Cadre) Area (Figure 1) - 4 to 6 positions – who are primarily responsible for monitoring and controlling the ISS Payloads.

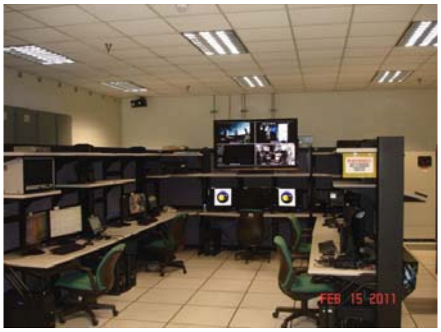

Figure 1. Cadre Area

- Integrated Support Team (IST) – 2 positions - who coordinate the planning and organizing of operational activities.
- Operations Support Team (OST) – 6 positions – who maintain HOSC systems in parallel with the HOSC operational network. The team consists of members from Network Management, Systems Management, and Database Management who maintain HPOC networks in parallel with the HOSC's network. During transition to HPOC, OST insure the HPOC systems are working as designed.

IV. HPOC Dependencies

HPOC is largely dependent on several unique elements of the HOSC to provide services. Most of these services are kept alive during planned events through generated power in the HOSC Demarcation area. These services are

- The highly qualified (low latency) ISS IP Ground Router (IIGoR) Network demarcation is in the HOSC. This provides Ku-Band as well as S-Band data from the ISS. As a result, the HPOC processors are co-located with the network access points.
- The Command Router interfaces between the HOSC and JSC are located in the HOSC. All Voice (T-1) Circuits are terminated in the HOSC. As a result, the Internet Voice Distribution System (IVoDS) for HPOC is co-located in the vicinity of the demarcation.
- The International Partner Gateway interfaces, as well as ground relays, are located in the HOSC.
- The HOSC Archive Library (HAL) is located in the HOSC, and is the ISS petabyte capable warehouse for Science Data storage and retrieval.

To achieve success in DR, these dependencies must be mitigated. These exist primarily as a result of engineering an environment to service short term goals, with a desire to achieve a long term Disaster Recovery concept. Funding is always instrumental, and it was made available expressly to accomplish the short term goal.

V. HPOC Lessons Learned

Many physical and architectural considerations were examined and optimized within the engineering process of HPOC. The lessons worthy of mention from our efforts are offered below, and are intended to assist others who desiring to develop or improve a DR concept.

A physically transportable concept proved to be very beneficial. It allowed the capability to locally test all sub-systems directly with operational systems. The opportunity to prove a working system locally and correct tedious configurations prior to move to the remote location was invaluable. The rack transportability concept included many provisions.

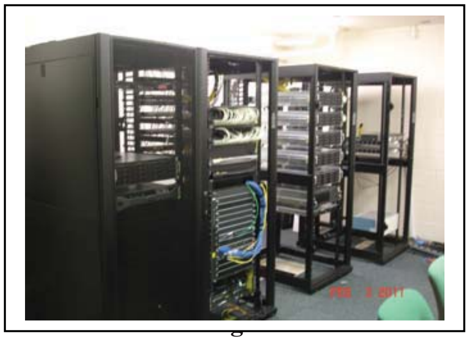

Figure 2. Rack Mount Flanges

Stabilization techniques for equipment deficient in mounting with both the front and rear mounting flanges of the rack. (Figure 2)

Patch panel connection schemes uniformly connecting all rack network connections from the top, forming a comprehensive patch connectivity scheme from a central network rack. (Figure 3)

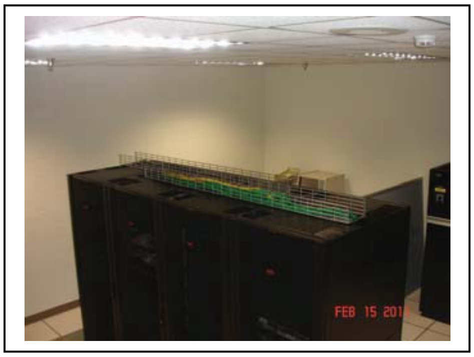

Figure 3. Top Mount Patch Panel Rack

With these accommodations, and a well-documented labeling nomenclature, the server environment was built and tested within the HOSC facility. Following engineering acceptance, the racks were transported to an alternate site with ease, connected, and ready for regression testing with our operational systems in less than 48 hours. (Figure 4)

Figure 4. Moving HPOC hardware and final setup

Also worthwhile to consider is the cluster voting schemes. The eviction logic of a Linux cluster manager can be optimized for the specific environment; however, other cluster technology may not offer the same latitude and control. This can influence node quantity, quorum requirements, and the network configuration. It is imperative that this logic is understood and accounted for within the system design.

Snapshot technology is an invaluable service for any DR capability. This concept allows system managers to present data as it was historically at a chosen point in time (pre-corruption, for example). Our most notable lesson learned in this area is the importance of a snapshot module capable of temporarily quiescing a rationale database during the process. This concept of integrity preservation is so important that Oracle offers its own independant solution branded "Dataguard," which the HOSC has successfully used on numerous occasions over the course of a decade.

One of the most valuable lessons without question relates to the use of cluster technology for both normal operations and contingency. Throughout architectural testing, and real-time operations, "Split brain" conditions are noteworthy risks. This is a condition in which a system or configuration loses the sense of resource ownership, resulting in inhibited services. For example, a cluster node may experience a condition in which it is locked out of storage resources by cluster intelligence.

While this is applicable to many firewalls, clusters, and various other concepts, Microsoft clusters were particularly susceptible to this condition for our environment. The preferred remediation for a split brain issue is to employ a primary/replica storage area network concept, whereby, in a planned scenario, a system manager performs a site failover or role reversal before bringing the disaster recovery node online. For our environment, we configured actual operational cluster nodes with a dual port host bus adapter within our DR environment. One port connects the node to the operational storage area network for day in/day out connectivity and operational participation. The secondary port allows the node connectivity to a disaster recovery storage area network. To fulfill this concept in a planned transition effort, a brief service outage is required. The cluster node in the disaster recovery environment is powered down while the SAN is subjected to a role reversal, making the disaster recovery environment the primary storage area network. The disaster recovery cluster node is then brought online whereupon it mounts its storage resources using the secondary adapter port dedicated for the DR SAN. In a planned event, the operational Logical Unit Number (LUN) would be presented and mounted in a true disaster recovery effort, inspection may dictate that a snapshot of this LUN be presented/mounted/used instead.

To normalize the configuration, the procedure is simply reversed. This method has been thoroughly tested and successfully used in our environment to support operations.

VI. Why an HPOC is Necessary?

Following a planned facility outage, complete system recovery is estimated to require in excess of 12 hours. Unplanned facility outages would normally require significantly more time depending on the circumstances. With the addition of HPOC, planned HOSC outages are nearly transparent to the end user; however, unplanned outages pose a very unique set of challenges.

The Tornado Outbreak of April 27, 2012, presented interesting challenges for norther Alabama, where the HOSC is located. Power was disrupted for nearly two weeks throughout northern Alabama, and for that duration the HOSC operated on generator power. This concept performed flawlessly, until power was unexpectedly interrupted for five minutes during one of the standard refill efforts. Considering the complex ground system and supporting infrastructure, the recovery effort from a power failure-- whether two seconds or two hours--is the same. The facility environmental control must be established and stabilized, the systems infrastructure must be recovered in a very specific order, split-brained resource ownership must be resolved, and data must be evaluated for corruption and backup recovery enacted as the circumstances warrant, and core ground system services must be reestablished and verified in a prescribed order.

While HPOC was not mature enough to compensate for the unplanned HOSC power failure, the environment did prove to be advantageous. Power to HPOC was uninterrupted, and core router responsibilities for both internal and external HOSC connections were kept alive by automatic transfer to the HPOC contingency. Additionally, all database logs were secure in the contingency environment, allowing for easy election of a current and credible centerpiece of the ground system. Combining these advantages with the expedited resuscitation of the HOSC environment, critical services were restored in less than seven hours.

VII. Conclusion

HPOC has succeeded in meeting the original objective well. The HPOC environment is in the midst of a transitional phase that is intended to modify the use case from a constantly used “hot” resource to a more valuable “warm” resource with a healthy capacity for comphrensive data retention complete with the ability to “roll back” file systems to a designated point in time. This concept increases the benefit of the envisioned future of the HOSC Logical Architecture, which centers on centralized and stateless virtual images.

The HOSC is transitioning from a RedHat Kernel-based Virtual Machine (KVM) and Windows Hypervisor Infrastructure to a common VMWare Virtual Server Infrastructure (VSI) for many elements of the ground system infrastructure. HPOC is a logical extension of HOSC Mission Operations, and as a result, will naturally inherit a respectable complement of VSI in parallel with operations. This evolution will strengthen the abilities of contingency operations through improved efficiency inherent with virtualization technology. This design is complete with snapshot retention of not only shared data, but also of the virtual machine images which create and manage it. Regardless of geographic location, virtualization greatly improves the operational concept of the contingency environment, as well as the transition plan for both planned and unplanned events.

The future vision of our Alternate Control Room/Disaster Recover area includes an aggressive virtualization model--a virtualized network, centralized storage, and a respectable percentage of virtualized servers. A dedicated Point-of-Presence for the unique HOSC circuits would reduce the dependencies on the HOSC and promote the logical architecture philosophy of parallel Ku and S-Band telemetry processing to a degree of alternate source. Storage will be enhanced to capture as-built data, as well as 45 days of change data, allowing true contingency operations with the ability to forensically interrogate historical configurations to better support root cause analysis. When the environment matures to this level, a permanent geographical location can be established with peering points to maximize the return on investment

Acknowledgements

This work was supported by NASA Marshall Space Flight Center Contract NNMO4AAO7C, Huntsville Operations Support Center.

References

[1] Telecommunications Industry Association (TIA), TIA-942, Data Center Requirements

[2] Alpha Magnetic Spectrometer (AMS) Project, http://ams.nasa.gov/index.html and http://www.ams02.org/