A Flexible Control Center Architecture for Support of Diverse Spaceflight Missions

Joan C. Differding[1]
NASA Ames Research Center, Moffett Field, CA, 94035, USA

Brian P. Stamper[2]
Logyx, Incorporated, Mountain View, CA, 94040, USA

The Ames Multi-Mission Operations Center (MMOC) enables and supports flight and science operations for Ames' spaceflight missions. The MMOC is composed of the facilities, networks, information technology equipment, software, and system administration services needed by flight projects to effectively and efficiently perform all mission functions, including planning, scheduling, command, telemetry processing, and science analysis. The MMOC's ready-to-use services reduce start-up time, shorten procurement and provisioning and allow mission planning efforts to focus more on science and less on infrastructure. The architecture of the MMOC was designed from the start for flexibility, so that it can readily support multiple missions of greatly varying size and complexity while simultaneously keeping costs low.

I. Nomenclature

ASIST	=	Advanced Spacecraft Integration & System Test Software
ATO	=	Authority To Operate
FISMA	=	Federal Information Security Management Act
IRIS	=	Interface Region Imaging Spectrograph
ITOS	=	Integrated Test and Operations System
LADEE	=	Lunar Atmosphere and Dust Environment Explorer
LAN	=	Local Area Network
LCROSS	=	The Lunar Crater Observation and Sensing Satellite
MMOC	=	Multi-Mission Operations Center
MOC	=	Mission Operations Center
MSA	=	Mission Specific Appendix
MSE	=	Mission Support Engineer
NASA	=	National Aeronautics and Space Administration
OASIS	=	Operations and Science Instrument Support
POC	=	Payload Operations Center
SOC	=	Science Operations Center
SOFIA	=	Stratospheric Observatory for Infrared Astronomy
SPHERES	=	Synchronized Position Hold, Engage, Reorient, Experimental Satellites
STP	=	Space Test Program
TAA	=	Trade Agreements Act
USAF	=	United States Air Force
VPN	=	Virtual Private Network

II. Introduction

NASA's Ames Research Center has successfully designed, built and flown a number of spacecraft, both small and large, dating back to Pioneer in the 1960s. In recent years, Ames has flown a variety of spaceflight missions, including the LCROSS, Kepler, LADEE and IRIS missions. In addition, it also supports operation of ISS payloads and science instrumentation, such as experiments using ESA's EMCS and technology demonstrations like SPHERES. The Ames

[1] Director, Multi-Mission Operations Center, Engineering Directorate.
[2] Information System Security Officer, Multi-Mission Operations Center, Engineering Directorate.

Multi-Mission Operations Center (MMOC) was created with the goal of increasing the efficiency of mission support activities and reducing the over-all cost of that support. The MMOC provides the facilities, networks, information technology equipment, software, and system administration services needed by flight projects to perform mission functions and relieves the missions of the burden of procuring and provisioning those things themselves. Because of the diverse nature of the spaceflight missions operating at NASA Ames, the MMOC is challenged to meet the needs of projects that vary in size, complexity and purpose. In this paper, we will describe how we designed and implemented a network architecture to support these disparate mission characteristics and how we structured and manage our information system security plan to document each mission's unique requirements, without becoming unwieldy or expensive.

Fig. 1 MMOC Control Center

III. Heterogeneous Customer Base

The operations roles that are performed at Ames vary greatly in size, complexity and purpose, and they have differing requirements for security and data handling. Spaceflight operations roles can be roughly grouped into three categories (Fig. 2):

- Mission operations: Commanding and controlling spacecraft
- Science operations: Managing science data pipelines and science data product generation
- Payload operations: Operating spacecraft payloads, both science experiments and technology demonstrators

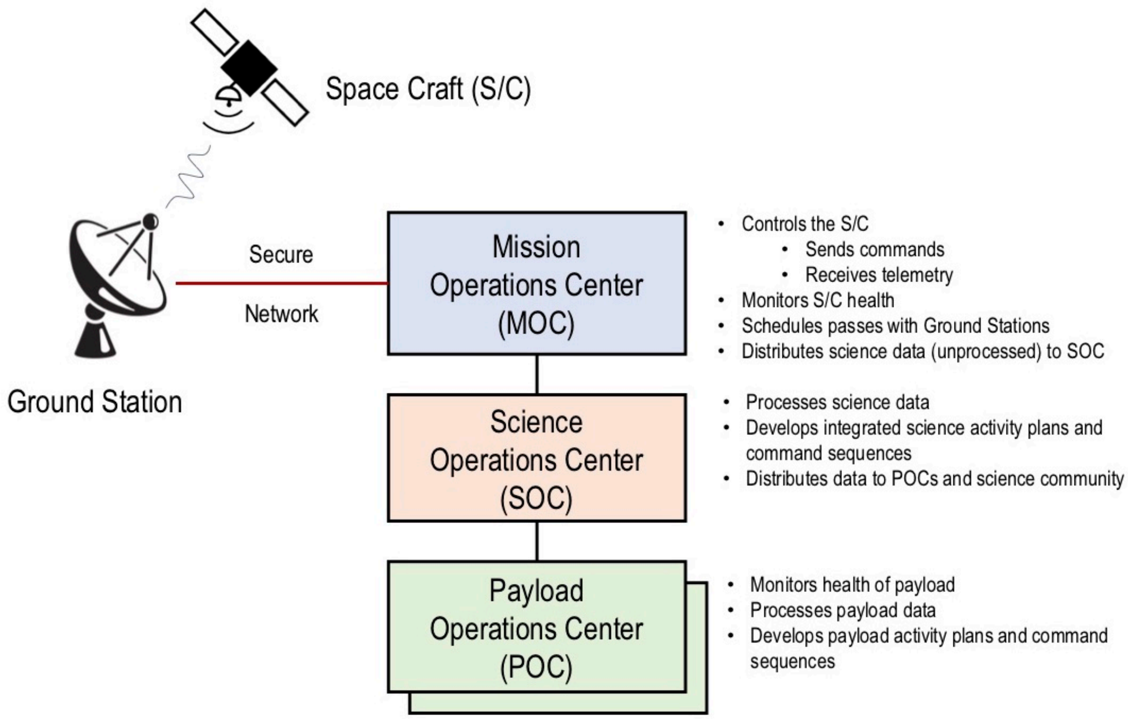

Fig. 2 Spaceflight operations roles

For any given mission, any combination of one or more of the roles may be performed at Ames (Table 1). The largest projects in the MMOC include the science operations center of the Kepler / K2 mission and the science network of the Stratospheric Observatory for Infrared Astronomy (SOFIA) Airborne Observatory. These projects feature complex science data pipelines that require large storage and compute power capabilities. The requirement for integrity of the data is high in order to ensure that the conclusions based on the data are high quality and reproducible. The availability requirement is low because analysis of science data is typically not a time critical process, and the confidentiality requirement is also low because of the desire to share science data and results across the scientific community. STPSat-5 is a US Air Force (USAF) mission for which Ames is providing mission operations services. In contrast to Kepler / K2 and SOFIA, STPSat-5 does not need large storage or compute power capabilities, but it does require high availability of the spacecraft telemetry in order to command the vehicle and monitor its health and high confidentiality to ensure exclusive use of the data by the USAF and its Department of Defense collaborators.

Table 1 Mission Roles and Characteristics

Project	Mission Ops	Science Ops	Payload Ops	Data Storage	Integ.	Avail.	Confid.
IRIS	✓			↑	↑	↑	↓
ISS Payloads			✓	↓	↑	↓	↑
Kepler / K2		✓		↑	↑	↓	↓
LADEE	✓		✓	↓	↑	↑	↑
LCROSS	✓	✓	✓	↓	↑	↑	↑
SOFIA		✓		↑	↑	↓	↓
STPSat-5	✓			↓	↑	↑	↑

IV. Designing for Flexibility

Given the wide range of requirements across the supported missions, it became clear early on that we could not apply a "one size fits all" approach to the MMOC's architecture or its policies. Instead, we made a conscious decision to design for efficient flexibility so that we could accommodate disparate requirements with a minimum of effort and expense.

The MMOC can be thought of as a stack of elements, each of which can be designed for flexibility, resiliency and efficiency (Fig. 3).

<table>
<tr><td>Facilities</td><td>• Buildings and appropriately outfitted rooms suitable for conducting mission operations, simulations, and training exercises</td><td rowspan="5">Security Plan</td></tr>
<tr><td>Network</td><td>• Dedicated network with specialized connections to ground station networks, other NASA centers, industry and academic partners, with appropriate routing and configurations for bandwidth, availability and security</td></tr>
<tr><td>Hardware</td><td>• Computer systems and workstations, servers, displays, etc.
• Multi-channel mission voice system
• Multi-terabyte on-line storage
• Virtual environment</td></tr>
<tr><td>Software</td><td>• Command and telemetry display and analysis software and tools
• Data management environments
• Analysis and planning tools
• Configuration management and verification and validation environments, tools to ensure compliance with NASA and Center software development and maintenance standards</td></tr>
<tr><td>Services</td><td>• System administration of mission environments (hardware and software)
• Management of data storage and archival services, including short-term data backup services and long-term data archive and retrieval services
• Security services (FISMA compliance, security model design)
• Requirements development and review support</td></tr>
</table>

Fig. 3 MMOC Elements

To determine suitability of the MMOC for a specific mission, the MMOC director meets with the mission representatives and discusses the following topics:

- Time and duration of the mission and the phases requiring MMOC support
- Spacecraft communication protocols and the desired command and telemetry handling software
- Functions that will be performed in the MMOC (for example: development, testing, orbital determination, spacecraft engineering, spacecraft commanding, receipt and storage of telemetry, science data processing, etc.)
- Size of project staff
- Critical operations periods and requirements for after-hours support
- Network connectivity with ground stations and project collaborators
- Classification of project data products and security requirements

Based on the discussion, the MMOC customer agreement is developed to formalize the plan for MMOC support. The customer agreement captures the mission's requirements for each of the MMOC elements.

A. Facilities

The first layer of the stack is the facility within which operations take place. This includes the physical rooms and their electrical, temperature control and security infrastructure. The MMOC does not have its own building dedicated to mission operations; instead the MMOC facilities are composed of sets of rooms (including server rooms) in several different buildings. For each set of rooms, the electrical system has been modified to meet the power requirements of the equipment housed there, and also to use circuits that automatically switch to power provided by a diesel generator in the event of a failure of the main electrical service. Dedicated heating, ventilation and air conditioning (HVAC) systems are deployed in the MMOC server rooms, and they are also powered by circuits that have backup generator coverage. If the main power were to fail, the generator starts up automatically and keeps all MMOC systems running and cool.

Physical security for the MMOC facilities is controlled with smartcard readers. The employee badges issued by NASA contain chips that can be read by Lenel smartcard readers for the purpose of unlocking the doors. Access is granted on an individual basis for specific rooms after completing a web-based workflow approval process that requires approval by the requestor's supervisor or project manager and by the MMOC director. This fine-grained approach to physical access allows the MMOC to provision entry to just the rooms that the requestor needs to perform his or her job, and no more, without much effort.

B. Network

When the MMOC was established, it was issued a segment of the NASA Ames corporate local area network (LAN) to manage for mission systems. Firewalls were put in place between the mission segment and the corporate LAN. All traffic leaving the MMOC LAN still had to traverse the corporate LAN to reach external parties. The agency virtual private network (VPN) services were also terminated on the corporate LAN. The result of this configuration was that traffic from dedicated circuits traversed a small segment of the corporate LAN without additional encryption or isolation. In addition, VPN traffic, intended to be encrypted, was only encrypted as far as the VPN concentrator, and would then flow unencrypted across the same small segment of corporate network on its way to the MMOC.

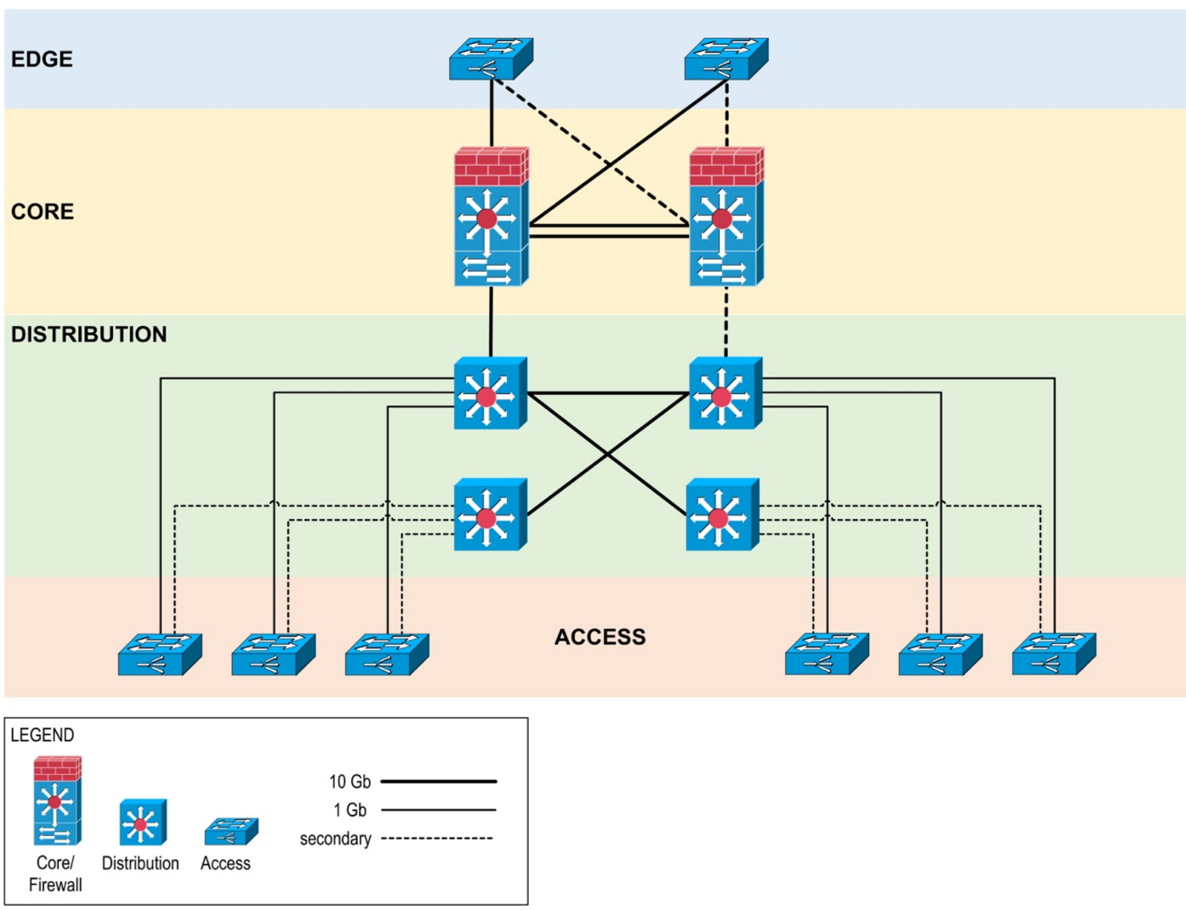

Fig. 4 Ames Mission Network Topology

Another issue created by sharing network resources with the corporate portion of the NASA Ames network was difficulties with maintenance scheduling. Mission services hours do not mesh well with an 8x5 corporate schedule. The demands of supporting the mission network made it very difficult for the corporate network group to perform enterprise maintenance. While they were willing to work around mission freezes and critical events, it would introduce delays of weeks or months to larger projects.

The design, as it was implemented, also included a lack of redundancy and several single points of failure. There was a single path from the corporate routers to the MMOC router, and single firewall appliances for each segment of network that the MMOC managed. The hardware itself was resilient, and there was never a major outage due to the design, but the possibility existed of a full network outage due to the failure of an individual device, power supply, cable, or network port.

To resolve these issues, the MMOC received approval and funding to establish its own fully managed network in 2011. This network was architected to provide 99.999% availability for the core of the network. Clustered pairs of routers, firewalls, and layer 2 distribution are located in two separate buildings, with geographically diverse fiber paths across campus connecting the core locations to the telco gateway (Fig. 4). All of the core network devices are housed in datacenters backed by both UPS and emergency generator power. The MMOC was granted its own autonomous system number and allowed to control the mission network out to its borders. This uncoupled the MMOC from center-wide corporate maintenance completely.

Other advantages to having a dedicated mission network include immediate turnaround time to implement approved firewall changes, the ability to span layer 2 networks across campus between mission operations locations, complete visibility into network issues without reliance on outside groups, the ability to ensure service levels for after-hours support, and the ability to establish secure end-to-end connections to external parties.

C. Hardware

The MMOC uses standard off the shelf server and network equipment. Whenever possible, we procure systems from a single vendor. This is useful for maintaining interoperability, as well as reducing complexity in system management. By utilizing a single vendor, it also saves effort on mandatory government checks on things like EnergyStar® and Trade Agreement Act (TAA) compliance.

In the past few years we have started to migrate away from discrete servers to an enterprise virtual environment. A virtual environment has several benefits. We can now quickly and efficiently deploy systems to meet most application, service, or security requirements without any additional hardware purchase. Significant time savings are realized with this approach since purchasing hardware at the federal government can be a very lengthy process. There are multiple checks and approvals needed, any one of which can introduce a delay of days or weeks. Once approved, there is a competitive bid process that must be undertaken for nearly all purchases. This process introduces further delays and cost; and can also result in errors as resellers don't always match exactly what the original purchase request contained. With the virtual infrastructure in place, we can more readily predict when we will need additional resources and plan ahead for the lengthy procurement cycle.

With an enterprise VMware® [1] environment in place, we are able to use vMotion™ to migrate systems between the hypervisors to perform maintenance on the underlying hypervisors without service interruptions. We are also able to use the high availability features within the VMware suite to increase availability for services that require it.

D. Software

The MMOC philosophy is to remain vendor neutral for software. As long as the software and operating system meet both the project's requirements and the MMOC's security requirements, each project is free to make its own decisions as to what software it uses. There are significant benefits to be realized through this approach, especially with the choice of command and telemetry software. Use of the same software in operations that was used during integration and test affords a significant reduction of risk compared to using a new software product and having to import the data dictionary from one application to the other. In the latter situation, any test results generated during integration and test are invalidated by changing to a new tool during operational readiness tests, so more extensive and costly tests must be run in order to verify that the new ground system software communicates appropriately with the flight software. In addition, potential errors in data translation represent a non-trivial threat to safe operation of the spacecraft. Often the choice of command and telemetry software is driven by the spacecraft developer, and in these cases, the project saves time and money and lowers their risk through this approach. However, there is a cost to this strategy in that the MMOC must hire system administrators who have a broad range of skills (e.g., can administrate a variety of operating systems) and can quickly learn how to manage new tools. The software applications supported by the MMOC to date are shown in Table 2.

Table 2 MMOC-Supported Software

Service	Function	Tool
Command and Telemetry	Commanding and telemetry display	ASIST [2], InControl [3], ITOS [4], OASIS-CC [5], TReK [6]
Voice System	NASA standard mission voice services	MOVE [7], IVoDS [8]
Flight Dynamics	Trajectory determination, orbital determination, attitude planning	STK [9], ODTK [10]

A number of tools are provided to all MMOC-supported projects for performing routine tasks (Table 3). The availability of these applications saves the missions the cost of licensing fees and also provides a common framework for conducting business in the MMOC. If a particular tool is not of general use, but more than one mission would like to use it, then the MMOC offers those missions the opportunity to cost-share to reduce expenses. All software proposed for use in the MMOC is evaluated by the MMOC's change control board for security issues and ease of maintenance before it is installed in the MMOC environment. Although not strictly enforced for business applications, customers are encouraged to use software that is already approved for use in the MMOC rather than requesting new tools that duplicate existing functionality.

Table 3 MMOC-Provided Applications

Service	Function	Tool
Directory service	Centralized system authentication	OpenLDAP [11]
Bug and issue tracking	Tracking of software bugs, MMOC support requests, and system change requests	Jira [12]
Real-time continuous system monitoring	Monitoring and alerting services for servers, switches, and applications	NAGIOS [13]
Configuration management and versioning	Source code repository; versioning of software deployments and system configurations	Subversion® [14], Git™ [15]
Wiki	Web-based, team collaboration	Confluence [16]
Instant Messaging	Quick communication	OpenFire [17], Pidgin [18]
License Server	Management of floating licenses	FLEXlm [19]
Backup and Archive	Encrypted backup of all system data to tape	NetWorker [20]
Analytical tools	Numerical computation environments	MATLAB® [21], IDL [22]

E. Services

When a mission operates out of the MMOC, it gains the advantage of support from the full MMOC staff of system administrators, database administrators, network engineer, and security specialist while only paying a fraction of those persons' salaries. The MMOC staff have experience supporting missions; and are able to assist in efforts including requirements development, the software development lifecycle, verification and validation, and change control. This background in mission support enables the MMOC staff to take a limited set of requirements from a mission and help to complete the overall mission architecture. In addition, the MMOC staff are cross-trained across missions and technologies so they may fill in for each other. Thus, the mission will not experience any lack of support due to someone on the MMOC team's being out sick or on vacation.

F. Security

The MMOC is a moderate-level system governed by the Federal Information Security Management Act (FISMA). The MMOC System Security Plan is designed to facilitate the ephemeral nature of the missions the MMOC supports. The foundational document provides information about the static elements and components of the environment, including the details related to the implementation of system-wide controls. Attached to the core security plan are Mission Specific Appendices (MSAs) that describe the security requirements and implementation for each mission. MSAs are intended to capture the unique characteristics of each mission in system-security-relevant terms (hardware and software inventory, network connectivity, system interconnections and any variances or additional requirements to the Moderate set of NIST and NASA security controls). As each new mission moves through the feasibility, concept, design, construction, testing and, eventually, mission operations support, the MSA is updated.

There are several advantages to this approach. There is a significant amount of up-front effort involved in creating a System Security Plan for a new information and subsequently maintaining the supporting documents. By centralizing this effort, we are able to reduce a great deal of redundancy between missions. Creation and maintenance of a security plan also requires a good deal of specific knowledge about compliance and the authorization to operate (ATO) process. This knowledge is not a skillset that would typically be found in mission-support personnel.

When a new system security plan is created, it must initially be audited and reviewed by an authorizing official and others before being granted an ATO. This process can take several months and incur significant expense. On the recent LADEE mission, Ames partnered with Goddard Space Flight Center, who provided the science operations center (SOC) for the program. Despite only requiring a handful of systems to operate the SOC, they were forced to create a system security plan from scratch, go through an internal audit, and receive an ATO for the system. This process took months, during which we were not permitted to establish network connectivity to the SOC from the MMOC. With the MMOC's flexible security plan structure, we are able to bring in a new project under our umbrella and avoid the need for this audit and ATO review. This strategy works because the overall approach the MMOC takes to handling mission systems has already been reviewed and approved. Minor exemptions and deviations to these processes are permitted and are captured within the MSA. The process to bring a small project the size of the LADEE SOC into the MMOC could have been accomplished in a few days.

Another advantage to the MMOC's security plan structure is the size of the environment and the complexity already present. When an information system makes a "significant change" to their environment, this can trigger a reassessment of their ATO. For a small mission, a significant change can be a fairly low threshold. With the MMOC's combining missions into one information system, most of the modifications an individual mission would enact would not approach the significant change threshold of the information system as a whole. Avoiding a reauthorization in this way saves time, effort, and cost.

One downside to this shared approach is a lack of flexibility to deal with lower security data. Since the MMOC handles moderate data, as defined by FIPS 199, the entire system is held to the moderate standard. This can cause some mission systems to be managed to a higher standard of security than would otherwise be required by their mission content. For the most part the additional effort is manageable, but it is a concern for some potential MMOC customers.

V. Conclusion

At NASA Ames Research Center, where small spaceflight missions are the norm, a multi-mission operations center is critical for individual missions to gain access to the equipment and services they need. A large mission may be able to afford to hire their own system or database administrators and buy their own equipment and software licenses. However, most do not have the means implement a dedicated network or make facility modifications, and they would prefer to avoid the expense of developing their own security plan. For small missions, all of these things are cost prohibitive. The MMOC enables small missions to fly with top-quality equipment and software in a secure environment and receive dedicated support for their systems. Our deliberate approach to designing for flexibility allows us to meet all the needs of our supported projects, without forcing them to compromise with a "one size fits all" solution, while maintaining a low price point.

VI. Acknowledgments

The authors would like to acknowledge their colleagues at Ames Research Center who contributed to the design of the MMOC:

Mark Foster, who designed the Ames Mission Network.

Mike Nelson, who pioneered the Mission Specific Appendix concept.

Robert Dumais, who founded the MMOC at NASA Ames Research Center.

All of our colleagues on the MMOC team over the years.

VII. References

[1] VMware®, Software Package, VMware, Palo Alto, CA, 2018.
[2] ASIST, Advanced Spacecraft Integration and System Test Software, Software Package, NASA Goddard Space Flight Center, Greenbelt, MD, 2012.
[3] InControl™, Software Package, L3, San Diego, CA, 2018.
[4] ITOS, Integrated Test and Operations System, Software Package, NASA Goddard Space Flight Center, Greenbelt, MD, 2018.
[5] OASIS-CC, Operations and Science Instrument Support Command and Control, Software Package, Laboratory for Atmospheric and Space Physics (LASP), Boulder, CO, 2018.
[6] TReK, Telescience Resource Kit, Software Package, NASA Marshall Space Flight Center, Huntsville, AL, 2018.
[7] MOVE, Mission Operations Voice Enhancement, Software and Hardware Package, Frequentis Corporation, Columbia, MD, 2018.
[8] IVoDS, Internet Voice Distribution System, Software Package, NASA Marshall Space Flight Center, Huntsville, AL, 2018.
[9] STK, Systems Tool Kit, Software Package, Analytical Graphics, Inc., Exton, PA, 2018.
[10] ODTK, Orbit Determination Tool Kit, Software Package, Analytical Graphics, Inc., Exton, PA, 2018.
[11] OpenLDAP, Software Package, OpenLDAP Project, Minden, NV, 2018
[12] Jira, Software Package, Atlassian, Sydney, Australia, 2018.
[13] NAGIOS, Software Package, Nagios Enterprises, Saint Paul, MN, 2018.
[14] Subversion®, Software Package, Apache™ Software Foundation, Wakefield, MA, 2018.
[15] Git, Software Package, Open Source, 2018
[16] Confluence, Software Package, Atlassian, Sydney, Australia, 2018.
[17] OpenFire, Software Package, Apache™ Software Foundation, Wakefield, MA, 2018.
[18] Pidgin, Software Package, Pidgin, 2018.
[19] FLEXlm, Software Package, Flexera Software, Dallas, TX, 2018.
[20] NetWorker, Software Package, Dell EMC, Hopkinton, MA, 2018.
[21] MATLAB, Software Package, MathWorks, Natick, MA, 2018.
[22] IDL, Interactive Data Language, Software Package, Harris Geospatial Solutions, Broomfield, CO, 2018.