NASA Integrated Network COOP

Michael L. Anderson[1] and Nathaniel Wright[2]
NASA/Goddard Space Flight Center, Greenbelt, Maryland, 20771

and

Wallace Tai[3]
NASA/Jet Propulsion Laboratory/California Institute of Technology, Pasadena, California 91109

Natural disasters, terrorist attacks, civil unrest, and other events have the potential of disrupting mission-essential operations in any space communications network. NASA's Space Communications and Navigation office (SCaN) is in the process of studying options for integrating the three existing NASA network elements, the Deep Space Network, the Near Earth Network, and the Space Network, into a single integrated network with common services and interfaces. The need to maintain Continuity of Operations (COOP) after a disastrous event has a direct impact on the future network design and operations concepts. The SCaN Integrated Network will provide support to a variety of user missions. The missions have diverse requirements and include anything from earth based platforms to planetary missions and rovers. It is presumed that an integrated network, with common interfaces and processes, provides an inherent advantage to COOP in that multiple elements and networks can provide cross-support in a seamless manner. The results of trade studies support this assumption but also show that centralization as a means of achieving integration can result in single points of failure that must be mitigated. The cost to provide this mitigation can be substantial. In support of this effort, the team evaluated the current approaches to COOP, developed multiple potential approaches to COOP in a future integrated network, evaluated the interdependencies of the various approaches to the various network control and operations options, and did a best value assessment of the options. The paper will describe the trade space, the study methods, and results of the study.

I. Introduction

National Aeronautics and Space Administration (NASA) Space Communications and Navigation (SCaN) Integrated Network Architecture Trade Studies were chartered by SCaN Management to respond to the SCaN Driving Requirement in the Program Commitment Agreement that calls for the development of a unified space communications and navigation architecture. The objective of the studies is to select the best-value architecture alternative that meets the objectives of the Integrated Network Architecture. This implementation of the new architecture will be realized through a phased approach[4]:

Phase 0: The As-Is Network represents the SCaN Network as it exists in 2010. In this phase, the SCaN Network is composed of three independent networks and their supporting functions.

Phase 1: The Pre-Integrated Network represents the SCaN Network in 2015. The three networks remain independent, add new capabilities that extend the functionality of the networks and address

[1] Network Systems Engineer, AIMM, Inc., NASA/GFSC Exploration and Space Communications Projects Division / Code 450, 8800 Greenbelt Road Greenbelt, Maryland 20771.
[2] Network Systems Integration Manager, NASA/GFSC Exploration and Space Communications Projects Division / Code 450, 8800 Greenbelt Road Greenbelt, Maryland 20771.
[3] Chief Engineer, NASA/JPL/Caltech Interplanetary Network Directorate, Mail Stop 126-200, Jet Propulsion Laboratory, 4800 Oak Grove Drive, Pasadena, CA 91109, USA.
[4] Space Communications and Navigation (SCaN) Network Architecture Definition Document, Volume 2 (ADD-V2)

upcoming mission needs. Furthermore, these new capabilities lay the groundwork for the next phase by beginning the implementation of key features of the Integrated Network, including standardized services and interfaces.

Phase 2: The Integrated Network represents the SCaN Network in approximately 2018. The three constituent networks are integrated into a unified C&N infrastructure by approximately 2018. This integrated network will be a single network consisting of NASA's C&N assets, presenting consistent, standardized services to user missions as well as providing new capabilities such as space internetworking.

Phase 3: The Post-Integrated Network represents the SCaN Network in approximately 2025. The capabilities of the integrated network are expanded further, infusing new technologies and answering the needs of NASA's long-term exploration and science goals.

Figure 1 illustrates the "should-be" architecture for Phase 2 of the effort which is planned to be realized by the 2018 era. While the overall architecture was divided into multiple studies for ease of managing the effort, the studies were closely coordinated and the interactions between the architecture options were closely monitored. Early in the process, it was determined that the Continuity of Operations (COOP) preparedness was tightly linked to every aspect of the architecture studies. This paper discusses the COOP study effort.

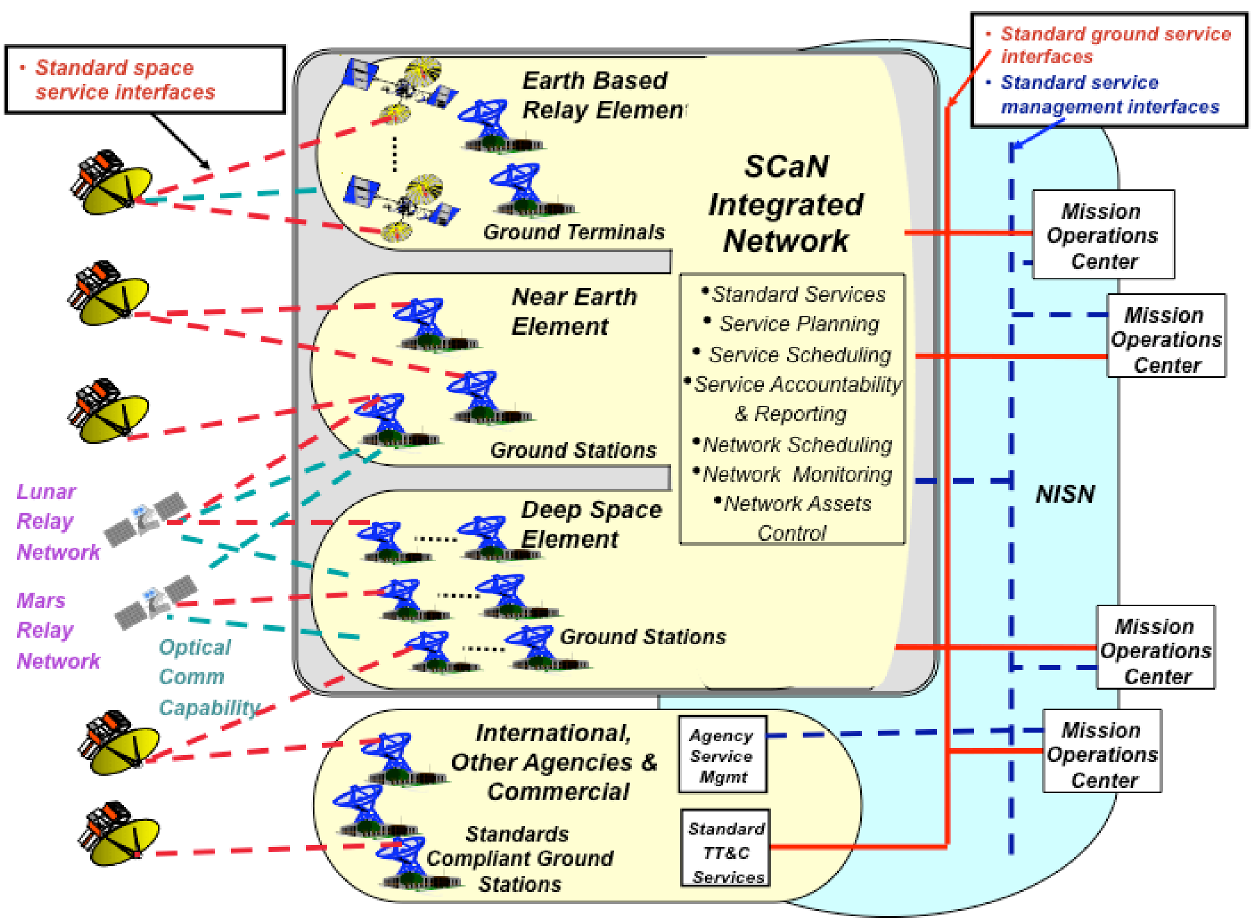

Figure 1: The NASA Integrated Network Architecture in 2018 establishes common user interfaces and enablers for infusion of future technologies

II. General

NASA Procedural Requirements (NPR) 1040.1[5] identifies the requirements to which NASA centers must adhere in regard to continuity of operations in the event of a disaster or other event that could disrupt mission-essential operations. These requirements are not meant to address day-to-day contingencies such as equipment failures or short term weather outages but are instead meant to address more catastrophic failures that could disrupt critical services for long periods of time.

NASA must have plans in place to ensure the performance of mission-essential operations during various types of emergencies or other situations that may disrupt normal operations. Specifically, mission-essential capability necessary to maintain the health and safety of space vehicles must be maintained. From a COOP perspective, collection of science data may have to be curtailed but infrastructure must be in place to prevent loss of a spacecraft and ensure safety of human life. NASA requirements stipulate that the contingency capabilities must be activated within twelve hours of an event and be capable of sustained operations for at least thirty days. The COOP plan must address facilities, equipment, and human resources necessary to maintain this level of preparedness.

III. Scope

The early stages of the study process determined that the integrated network will utilize a distributed service execution architecture. Thus the network elements, individually and/or in combination, will provide inherent redundancy for service execution capabilities. COOP is one of the driving factors in that decision. A more centralized approach would require back-up facilities that are not required in a distributed system. This would add cost for facilities, equipment, and staffing. In a distributed system a catastrophic failure at one location will confine service interruption to a limited number of users. This strategy significantly reduces the impact of a COOP event. Hence service execution is not addressed in this study.

In addition a key requirement for the Integrated Network is that it will use internationally recognized standards wherever possible. Therefore the generally accepted and widely implemented Consultative Committee for Space Data Systems (CCSDS) standards will be utilized wherever practical. By providing standardized interfaces users can access resources to meet their needs relatively seamlessly among the three network elements. Users can also utilize international and commercial agency assets that support the same standard interfaces. This interface standardization enhances the COOP posture of the integrated network.

This study does not include assessments of threats that might cause a COOP event. Rather the study assumes a COOP event to be anything that would disable a complete facility for an extended period of time. This approach produces a strategy that addresses the unknown as well as the known.

IV. Requirements

NPR 1040.1 was evaluated to identify requirements for the future Integrated Network Architecture and to identify any gaps in the existing architecture. The following requirements were considered the driving requirements from a SCaN perspective:

> 30012 As a baseline for preparedness, NASA Headquarters and NASA Centers are required to have in place a viable COOP capability that ensures the performance of their mission-essential operations during any type of emergency, or other situation that may disrupt normal operations.
>
> 30013 A viable COOP capability must (1) be maintained at a high level of readiness; (2) be capable of being implemented with and without warning; (3) be operational within 12 hours of activation; (4) maintain sustained essential operations for a minimum of 30 days; and (5) take maximum advantage of available field infrastructure, existing Agency emergency preparedness program procedures, and established Information Technology (IT) Security plans.

[5] NASA Procedural Requirements (NPR) 1040.1 – NASA Continuity of Operations (COOP) Planning Procedural Requirements w/Change 3 (03/30/05) (NPR 1040.1)

30090 Centers will use the following criteria when making COOP judgments. These criteria will serve to identify essential operations that require development of COOP:

a. Would the loss of a Center MEI capability or operation compromise national security?
b. Would the loss of a Center mission-essential infrastructure capability or operation have an immediate and significant adverse effect on the health and safety of the general public at large?
c. Is a NASA Center mission-essential capability or operation critical to the performance of another agency's COOP essential operations and required, by agreement, to remain viable, without interruption, under all emergency conditions?
d. Is the NASA mission-essential capability or operation regulated, legislated, or directed by Executive order to operate under all emergency scenarios?
e. Is the mission-essential capability or operation tied into a space exploration vehicle and equipment command and control operations that if rendered inoperable, would place personnel, vehicles and/or equipment at risk? Would the cost to recover from such an event exceed NASA's budget capability?
f. Is the mission-essential capability or operation a deemed vital service, as determined by NASA management and, therefore, required under COOP?

Most SCaN Network assets fall under category “e”. It is noteworthy that this criterion relates to capabilities required to avoid placing “personnel, vehicles and/or equipment at risk.” It does not necessarily include maintaining continuity of mission science or user data. This is an important consideration since it can be a significant cost driver. However, some SCaN assets or services may fall under other criteria which require continuity of user data in a COOP scenario. Thus each SCaN capability was reviewed on a case-by-case basis to determine the minimum capabilities required.

SCaN overall network requirements and individual network element requirements were derived from the NPR driving requirements. These have been incorporated in the SCaN Network System Requirements Document (SRD)[6].

V. Current COOP Approach

The current approach to COOP in SCaN is managed by each individual element. Each element relies on the diversity of ground stations and relay elements to provide COOP for service execution. They each have back-up capabilities within their respective elements for scheduling and network control. If a system is impacted by a COOP event, the network elements implement their own plans to restore service within their individual element. Some users can utilize multiple network elements and may request services from a different element if there is a failure in their normal element. It is the user’s responsibility to initiate the change. There is no current plan to address COOP from an overall SCaN network perspective.

A. Near Earth Element (NEE)

The NEE consists of geographically dispersed ground stations. Each ground station has one or more antennas with dedicated strings of radio frequency (RF) and data processing equipment. Missions supported by NEE can all be supported by more than one NEE station. NEE also exercises established contracts with commercial providers that have their own internal back-up capability. Furthermore most missions supported by NEE can also be supported by the Deep Space Element (DSE). In some cases the Earth Base Relay Element (EBRE) can provide levels of support to missions traditionally supported by NEE. NEE also has a reciprocal agreement with NOAA to provide back-up support. Because of the geographical diversity of the NEE stations and the ability to receive support from several other entities, a single event is not likely to cause a loss of ability to provide Telemetry, Tracking, and Control (TT&C) to any NEE-supported mission.

The NEE scheduling system does not have a geographically separate hot back-up system. Currently the NEE is scheduled using the Wallops Orbital Tracking Information System (WOTIS) system located at the NASA White Sands Complex in New Mexico. There is an additional WOTIS system at Wallops Flight Facility (WFF) in Wallops Island Virginia that is used for test and planning functions but it is not configured as a hot back-up to the operational

[6] Space Communications and Navigation (SCaN) Network System Requirements Document (SRD) Version 1 – Pre-Integrated Network Phase

systems. This system could be used to manually schedule contacts if necessary. This would satisfy the requirement to safeguard mission-essential operations.

The additional WOTIS system at Wallops could be configured as an operational back-up to provide a higher level of support during a catastrophic event. The effort to make the necessary changes is minimal and trained personnel are available to operate the system in an emergency. Implementing this additional operational back-up would put the NEE in a better posture in regard to COOP.

By Point-of-Departure (POD), circa 2018, NEE will have adopted a centralized Monitor and Control (M&C) approach where multiple stations are monitored and controlled from a central location at Wallops. When this occurs, the ground stations will have personnel on-call to operate locally when necessary. This is a viable approach as long as the trained personnel are available at all of the ground stations.

B. Deep Space Element (DSE)

The DSE has three Deep Space Communications Complexes (DSCCs) – Goldstone, CA USA; Madrid, Spain; and Canberra, Australia. These stations are geographically located to maximize coverage of deep space missions. Each DSCC has multiple Ground Stations that can, with some limitations, be used interchangeably. If a given event renders one or more antennas at a site inoperable, other antennas will provide support to the most critical activities being performed. Typically multiple antennas are tracking a mission simultaneously during critical events. If an event renders an entire ground station inoperable, critical missions can be supported by the other stations.

If a complete DSCC were inoperable, there would be some period of time when missions could not be continuously supported until the Earth's rotation brought one of the other stations into view of the space vehicle. In most cases this gap would not "place personnel, vehicles and/or equipment at risk", but there may be a loss of science data. Autonomous spacecraft operations minimize any potential for loss of missions even if there is a gap in continuous coverage.

Currently all of the data at a given ground station is demodulated and processed in a single building. RF signals are converted to optical signals and are sent to the Signal Processing Center (SPC) where the signals are processed using pooled equipment. This pooled approach has several advantages such as reduced equipment count and ease of maintenance, but there is an inherent risk in having all of the equipment at one location. Future architectures may consider locating some of the pooled resources at a second on-site location to minimize the potential of a single incident impacting the entire DSCC.

The DSE also has agreements in place with international partners to use their deep space networks if required. In addition to providing back-up to DSE assets, these networks provide coverage in geographic areas that are not covered by the existing DSCCs.

In addition to the ground stations, the DSE includes a central Network Operations Control Center (NOCC) which generates network schedules and pointing data and a Data Systems Operations Center (DSOC) located on the JPL campus in Pasadena, California. The NOCC and DSOC functions can be remotely operated from the Remote Operations Center (ROC) located in Monrovia, CA, a short distance from JPL. The Monrovia facility can be activated in less than 12 hours and can operate for well over thirty days. However, remote operations from the ROC depend on operational servers at the primary location. This limits utility as a back-up to scenarios where the primary facilities are uninhabitable but otherwise fully functional (power, communications, cooling, etc.).

If the NOCC at JPL were rendered inoperable, operations could be relocated to the Emergency Control Center (ECC) in Goldstone, CA. The ECC provides real-time, full-duplex data and voice communications capability with all three (DSCC) (at least 12Mb/s per complex), generation and transmission of DSE pointing and frequency predictions for the DSCCs, and limited recording and archiving of telemetry data received. Note: telemetry data is limited only to spacecraft engineering health and safety; processing of tracking data via the Radio Metric Data Conditioning (RMDC); generation of TRK-2-34 and TRK-2-18 Doppler Observables to allow post-pass high level assessment of tracking data quality; command transmission capability; interfaces with non-JPL mission control centers (e.g., Lockheed Martin Astrophysics) where communication links are available for telemetry, tracking, command, monitor data, and state vectors; and voice communication between the ECC and DSCCs via a dedicated international conference line. These capabilities, while limited, provide the communication capabilities with user spacecraft sufficient to maintain vehicle health and safety.

The ECC also provides space and facilities for user TT&C workstations. Provision and maintenance of these workstations and their operation is the user's responsibility and is not part of this study.

In addition to supporting deep space probes, the DSE provides several other functions to the science community including Very Long Baseline Interferometry (VLBI) and Radio Science. Based on NPR 1040.1 guidelines, coverage of these other functions are not to be considered mission-essential and will be given less priority than support to the deep-space probes.

C. Earth Based Relay Element (EBRE)

The EBRE has three terminals providing Tracking Data Relay Satellite (TDRS) TT&C and user services. Two of the terminals, the White Sands Ground Terminal (WSGT) and the Second TDRS Ground Terminal (STGT), are located near Las Cruces, New Mexico. These terminals support TDRS in the Atlantic Ocean Region (AOR) and the Pacific Ocean Region (POR). The third terminal, the Guam Remote Ground Terminal (GRGT), is located on the island of Guam. GRGT supports TDRS in the Indian Ocean Region (IOR). A fourth terminal is being developed at Blossom Point, Maryland. The Blossom Point TDRS facility will extend TDRS coverage in the AOR.

In addition to the antennas providing both user services and TDRS TT&C, the EBRE has several S-band only antennas that provide TDRS TT&C support. These antennas are not capable of providing user services. STGT and WSGT each have one S-band TT&C antenna. There are two additional S-band antennas at the Extended TDRS Ground Terminal (ETGT) at WSC. In addition to providing S-band connectivity to TDRS, ETGT has a stand-alone TDRS Real Time Monitoring Systems (RTMS) that can be used to provide standalone TDRS TT&C. Dedicated S-band support is also provided by the Australian TDRS Facility (ATF) at Dongara, Australia. The facility provides support for any POR and IOR TDRS when they are not in view from White Sands. These dedicated S-band antennas are used to maintain in-orbit spares and for contingency support.

WSC can also utilize external S-band assets when necessary. This includes the DSE 34 meter antennas and select NEE antennas. In general, the external systems are only used for emergency support.

For COOP purposes, STGT and WSGT are considered as back-ups to each other. In a COOP scenario where one of the facilities is rendered inoperable, the remaining site would be used to maintain the TDRS fleet and support limited user services.

If STGT or WSGT fails, the remaining station could support user services and provide TDRS TT&C using available Space to Ground Link Terminals (SGLT)s. In addition, the S-band antennas at WSC can be used to maintain health and safety of up to three TDRS. If required, external S-band assets (NEE and DSE) could be utilized through either STGT or WSGT.

If an event occurred that rendered Guam inoperable, the IOR TDRS TT&C operations could be performed using ATF or external S-band antennas. User services, however, would not be available from Guam. Other TDRSs could be rescheduled to provide critical support for missions that can be seen by multiple TDRSs but platforms that are only in view of IOR TDRSs could not be serviced. In addition, any local user interfaces or equipment that is unique to Guam could not receive data from White Sands.

A number of limitations to the current COOP posture were identified by this study. The details are beyond the scope of this discussion. These limitations are currently being addressed. The implementation of the SN Ground System Sustainment (SGSS) project and the new ground station at Blossom Point will result in a significant enhancement to the EBRE COOP posture.

VI. COOP Architecture Alternatives

Based on the requirements and evaluation of current gaps, three COOP options were developed for the future SCaN Integrated Network. The options are described in Table 1 below.

Table 1 – SCaN Integrated Network COOP Options

OPTION	DESCRIPTION
COO-1 Cross support backup between network elements	Each network element (EBRE, NEE, or DSE) relies on another network element to provide backup capabilities for network control in time of disastrous events for maintaining COOP. This implies, for network control functions, a Network Operations Node (NON) hosts or serves as the backup NON for another network element.
COO-2 Central back-up	A single site, at a geographical location different from any of the NONs for the three network elements, provides backup capabilities for network control to all network elements in time of disastrous events for maintaining COOP.

OPTION	DESCRIPTION
COO-3 Self confined backup at each network element	Each network element (EBRE, NEE, or DSE) provides backup capabilities for network control by itself within its own system and performs backup activities in time of disastrous events for maintaining COOP. No cross-support among network elements takes place. This implies within each network element there exists a backup site hosting or serving as the backup NON.

System Context - Figure 3 shows the options in context.

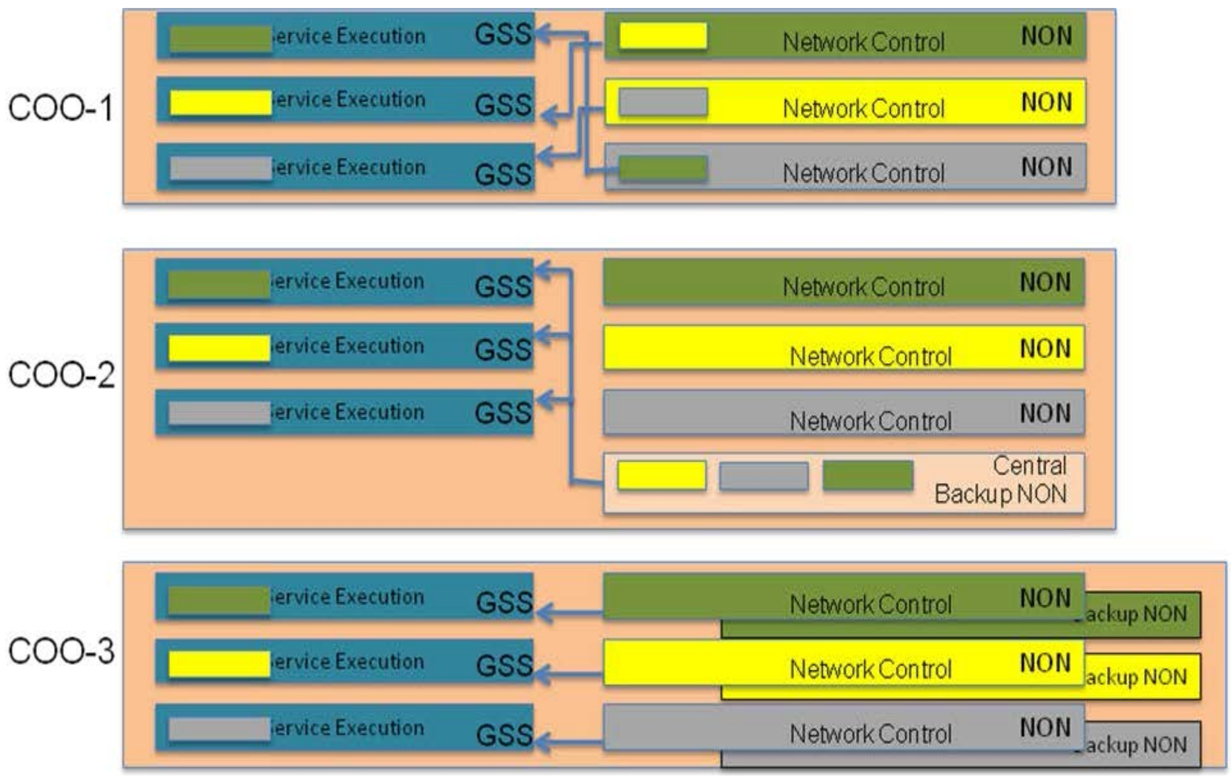

Figure 3 – SCaN Integrated Network COOP Study Context Diagram

Coop Option Implications - In the Integrated Network context, the COOP options have differing implications on the system design. These implications are shown below.

A. COO-1 Cross Support Backup between Network Elements

- Network control functions at a given element NON are supported from a different element NON in time of disastrous events.
- A backup NON must host sufficient equipment to provide mission essential operations.
- Network control personnel at a backup NON must be trained to support both elements OR those at the primary NON must travel within an achievable and committed number of hours to the backup NON to conduct network monitor and control operations.

- A backup site must have same personnel and facility clearance levels as the primary site.
- Specialized network control functions, e.g., TDRS TT&C may require backup within an element due to unique skills.

B. COO-2 Central Back-Up

- Network control functions at each element NON are supported from a central backup NON in time of disastrous events.
- The backup NON must host sufficient equipment to provide mission essential operations for each network element.
- The central backup NON must be staffed by trained personnel to support each network element OR those at each network element NON must travel within an achievable and committed number of hours to the backup NON to conduct network monitor and control operations.
- The central backup site must have same personnel and facility clearance levels as the highest level primary site.
- Specialized network control functions, e.g., TDRS TT&C may require backup within an element due to unique skills.

C. COO-3 Self Confined Backup at Each Network Element

- Network control functions at a given element NON are supported from a backup NON within the network element in time of disastrous events.
- The backup NON must host sufficient equipment to provide mission essential operations.
- Operations personnel at the backup NON site must be trained to perform network monitor and control operations OR those at the primary NON must travel within an achievable and committed number of hours to the backup NON to conduct operations.
- The backup site must have same personnel and facility clearance levels as the primary site.
- Specialized network control functions, e.g., TDRS TT&C may require backup within an element due to unique skills.
- No operations personnel will require cross-training to support other network elements.

VII. Software Design Implications

These implications impact the various software designs in different ways. This is shown in Table 2. From a cost perspective it is important to note that the main cost of COOP is additional instantiations of hardware and software. Thus the main difference between the options is the location of the equipment to be installed, not the quantity of equipment. Hence the cost differential of hardware and software between options is insignificant.

Table 2 – Integrated Network COOP Approach / Software Architecture Matrix

	COO-1 Cross-support backup between network elements	COO-2 Central back-up	COO-3 Self-confined backup at each network element
Network Control Systems (NCS)-1 through NCS-4	Software/databases at each back-up facility must be kept up-to-date. Routine proficiency passes must be done. Communications for each supported element must be provided and regularly tested.	Software/databases at each back-up facility must be kept up-to-date. Routine proficiency passes must be done. Communications for each supported element must be provided and regularly tested.	Software/databases at each back-up facility must be kept up-to-date. Routine proficiency passes must be done. Communications for each supported element must be provided and regularly tested.
NCS-1 Common network control framework	Sufficient hardware must be replicated at a back-up facility to support the element being backed up. A common framework minimizes training, but personnel must be trained in element-specific processes.	Sufficient hardware must be replicated at the central back-up facility to support all three networks, although not necessarily at the same time. A common framework minimizes training, but personnel must be trained in element-specific processes for all three networks.	Sufficient hardware must be replicated at each back-up facility. . Personnel must be trained in element-specific processes for supported network.
NCS-2 Common network control interface	Sufficient hardware must be replicated at a back-up facility to support the element being backed up. A common framework minimizes training, but personnel must be trained in element-specific processes.	Sufficient hardware must be replicated at the central back-up facility to support all three networks, although not necessarily at the same time. . A common framework minimizes training, but personnel must be trained in element-specific processes for all three networks.	Sufficient hardware must be replicated at each back-up facility. . Personnel must be trained in element specific processes for supported network.
NCS-3 Central gateway	The central Gateway must be replicated at each back-up NON. Network specific M&C hardware and software must be replicated at each back-up NON. . Personnel must be trained in element-specific systems and processes.	The central Gateway must be replicated at the central back-up NON. Network specific M&C hardware and software for each network must be replicated at the back-up NON.. Personnel must be trained in element specific systems and processes.	Sufficient hardware must be replicated at each back-up facility. Personnel must be trained in element specific processes for supported network.
NCS-4 Network element gateway	A central Gateway must be replicated each back-up NON. Network-specific M&C hardware and software must be replicated at each back-up NON. Personnel must be trained in element-specific systems and processes.	A central Gateway must be replicated the central back-up NON. Network-specific M&C hardware and software must be replicated at the back-up NON. Personnel must be trained in element-specific systems and processes.	Sufficient hardware must be replicated at each back-up facility. Personnel must be trained in element specific processes for supported network.

VIII. Conclusions

The various COOP options were evaluated along with the NCS options. The team first identified key figures-of-merit (FOM) that were considered important attributes of a new integrated network. These FOMs were then weighted by relative importance and scored on an option-by-option basis. Considerable effort was made to estimate the relative cost of each option. The technical merit of each option was then compared with the relative price and a best value judgment was used to determine the final recommendation.

NCS-1 coupled with COO-1 were chosen for the initial implementation of the integrated network. Through this approach the network control capabilities for each network element are inherently resident at another network element as this is the main essence of the network control software design of the NCS-1. This provides an inherent ability to achieve COOP in time of disastrous events. In addition, the operational proficiency at the supporting network element is maintained through the occasional cross support to the supported network element for network monitor and control operations. As stated earlier, a single COOP event will not prevent fulfilling minimum service execution requirements as the service execution elements (ground stations) will be geographically distributed. Instead, this study focused on the network control functions. Without adequate back-up a single event could render an entire network element inoperable. Using COO-1, each network element will be backed up by at least one other element. This will provide sufficient capabilities to meet the minimum COOP requirements.

Acknowledgments

The work was chartered and funded by the NASA SCaN Program Office. The strong and dedicated management support by Jim Schier, Phil Liebrech, and Badri Younes is appreciated. Part of the study was carried out at the JPL/Caltech, under a contract with the NASA.