2006-06

Rapid Response Command and Control (R2C2): a systems engineering analysis of scaleable communications for Regional Combatant Commanders

NPS-97-06-002

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

RAPID RESPONSE COMMAND AND CONTROL (R2C2): A SYSTEMS ENGINEERING ANALYSIS OF SCALEABLE COMMUNICATIONS FOR REGIONAL COMBATANT COMMANDERS

by

LCDR Lisa Sullivan
LT Lennard Cannon
LT Ronel Reyes
ENS Kitan Bae
ENS James Colgary
ENS Nick Minerowicz
Maj. Chris Leong
Maj. Harry Lim
Mr. Hang Sheng Lim
Ms. Chin Chin Ng
Capt. Tiong Tien Neo
Mr. Guan Chye Tan
Maj. Yu Loon Ng
Maj. Eric Wong
Mr. Heng Yue Wong

June 2006

Prepared for: Deployable Joint Command and Control (DJC2)
Joint Program Office
110 Vernon Avenue, Code DPJ
Panama City, FL 32407-7001

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2006	**3. REPORT TYPE AND DATES COVERED** Thesis Technical Report	
4. TITLE AND SUBTITLE Rapid Response Command and Control (R2C2): A Systems Engineering Analysis of Scaleable Communications for Regional Combatant Commanders			**5. FUNDING NUMBERS**
6. AUTHOR(S) LCDR Lisa Sullivan, LT Lennard Cannon, LT Ronel Reyes, ENS Kitan Bae, ENS James Colgary, ENS Nick Minerowicz, Maj. Chris Leong, Maj. Harry Lim, Mr. Hang Sheng, Ms. Chin Chin Ng, Capt. Tiong Tien Neo, Mr. Guan Chye Tan, Maj. Yu Loon Ng, Maj. Eric Wong, Mr. Heng Yue Wong			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-97-06-002
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Deployable Joint Command and Control (DJC2) Joint Program Office, 110 Vernon Avenue, Code DPJ, Panama City, FL 32407-7001			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT ***(maximum 200 words)***

Disaster relief operations, such as the 2005 Tsunami and Hurricane Katrina, and wartime operations, such as Operation Enduring Freedom and Operation Iraqi Freedom, have identified the need for a standardized command and control system interoperable among Joint, Coalition, and Interagency entities. The Systems Engineering Analysis Cohort 9 (SEA-9) Rapid Response Command and Control (R2C2) integrated project team completed a systems engineering (SE) process to address the military's command and control capability gap. During the process, the R2C2 team conducted mission analysis, generated requirements, developed and modeled architectures, and analyzed and compared current operational systems versus the team's R2C2 system. The R2C2 system provided a reachback capability to the Regional Combatant Commander's (RCC) headquarters, a local communications network for situational assessments, and Internet access for civilian counterparts participating in Humanitarian Assistance/Disaster Relief operations. Because the team designed the R2C2 system to be modular, analysis concluded that the R2C2 system was the preferred method to provide the RCC with the required flexibility and scalability to deliver a rapidly deployable command and control capability to perform the range of military operations.

14. SUBJECT TERMS Systems engineering, rapid communications, wireless technology, satellite communications, Combatant Commanders, humanitarian assistance, disaster relief, civil unrest, requirements, functional analysis, modeling, and analytic hierarchy process (AHP)			**15. NUMBER OF PAGES** 237
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA 93943-5001

RDML Richard Wells, USN
President

Richard Elster
Provost

This report was prepared for the Deployable Joint Command and Control (DJC2) Joint Program Office, 110 Vernon Avenue, Code DPJ, Panama City, FL 32407-7001.

This report was prepared by Systems Engineering and Analysis Cohort Nine (SEA-9) Rapid Response Command and Control (R2C2) team members:

LCDR LISA SULLIVAN, USN
LT LENNARD CANNON, USN
LT RONEL REYES, USN
ENS KITAN BAE, USN
ENS JAMES COLGARY, USN
ENS NICK MINEROWICZ, USN
Maj. CHRIS LEONG
Maj. HARRY LIM
MR. HANG SHENG LIM
MS. CHIN CHIN NG
Capt. TIONG TIEN NEO
MR. GUAN CHYE TAN
Maj. YU LOON NG
Maj. ERIC WONG
MR. HENG YUE WONG

Reviewed by:

JOHN OSMUNDSON, Ph.D.
SEA-9 Project Advisor

WAYNE P. HUGHES, JR.,
CAPT, USN (Ret.)
Chair, SEACC

Released by:

FRANK E. SHOUP, Ph.D.
Director, Wayne E. Meyer Institute of Systems Engineering

LEONARD A. FERRARI, Ph.D.
Associate Provost and Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Disaster relief operations, such as the 2005 Tsunami and Hurricane Katrina, and wartime operations, such as Operation Enduring Freedom and Operation Iraqi Freedom, have identified the need for a standardized command and control system interoperable among Joint, Coalition, and Interagency entities. The Systems Engineering Analysis Cohort 9 (SEA-9) Rapid Response Command and Control (R2C2) integrated project team completed a systems engineering (SE) process to address the military's command and control capability gap. During the process, the R2C2 team conducted mission analysis, generated requirements, developed and modeled architectures, and analyzed and compared current operational systems versus the team's R2C2 system. The R2C2 system provided a reachback capability to the Regional Combatant Commander's (RCC) headquarters, a local communications network for situational assessments, and Internet access for civilian counterparts participating in Humanitarian Assistance/Disaster Relief operations. Because the team designed the R2C2 system to be modular, analysis concluded that the R2C2 system was the preferred method to provide the RCC with the required flexibility and scalability to deliver a rapidly deployable command and control capability to perform the range of military operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

A

AES	Advanced Encryption Standard
AHP	Analytic Hierarchy Process
AOR	Area of Responsibility
ASG	Abu-Sayyaf Group

B

BAA	Broad Area Announcement
BDA	Battle Damage Assessment
BW	Bandwidth

C

C2	Command and Control
CAC	Common Access Card
CBR	Chemical, Biological, and Radiological
CDR	Critical Design Review
CENTCOM	Central Command
CENTRIXS	Combined Enterprise Regional Information Exchange System
CEP	Circle Error Probable
CI	Critical Infrastructure
CIE	Collaborative Information Environment
CJCS	Chairman of the Joint Chiefs of Staff
CMOC	Civil-Military Operations Center
CMS	Civil/Military Suite
COASTS	Coalition Operating Area Surveillance and Targeting System
COC	Combat Operations Center
CoDR	Conceptual Design Review
COI	Critical Operational Issue
COMLOGWESTPAC	Commander Logistics Western Pacific
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial-off-the-shelf
CPD	Capability Production Document
CRG	Contingency Response Group

D

DB	Data Base
DCTS	Defense Collaboration Tool Suite
DII	Defense Information Infrastructure
DJC2	Deployable Joint Command and Control
DoD	Department of Defense

DoS	Denial of Service
DTED	Digital Terrain Elevation Data

E

EMS	Emergency Medical Service
EoIP	Everything over IP
ESG	Expeditionary Strike Group
ETA	Estimated Time of Arrival
EUCOM	European Command

F

FBI	Federal Bureau of Investigation
FLAK	Fly-Away-Kit
FOB	Forward Operating Base

G

GB	Gigabytes
GCCS-J	Global Command and Control System – Joint
GEO	Geosynchronous Earth Orbit
GIG	Global Information Grid
GOTS	Government Off The Shelf
GSM	Global System for Mobile
GWOT	Global War On Terror

H

HA/DR	Humanitarian Assistance and Disaster Relief
HFN	Hastily Formed Networks
HSI	Human System Interface
HVT	High Value Target or (Terrorist)

I

IA	Information Assurance
IAEA	International Atomic Energy Agency
IATF	Information Assurance Technical Framework
I&A	Identification and Authentication
ID	Identification
IDS	Intrusion Detection Systems
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
ILS	Integrated Logistics Support
IM	Information Management
Info	Information
IO	International Organization
IP	Internet Protocol
IR	Infrared
ISP	Internet Service Provider

ISSE	Information System Security Engineering
IWS	Information Workstation
J	
JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JSIC EC2	Joint Systems Integration Command Executive Command and Control
JP	Joint Publications
JPO	Joint Program Office (for DJC2)
JTF	Joint Task Force
JTTP	Joint Tactics, Techniques, and Procedures
K	
Km	Kilometer
KMI	Key Management Infrastructure
L	
LAN	Local Area Network
LCD	Liquid Crystal Display
LEO	Low Earth Orbit
LHC	Long Haul Communication
LMR	Land Mobile Radio
LOC	Local Communications
LS	Local Suite
M	
MC	Medical Corps
MCT	Message Completion Time
MCR	Message Completion Rate
MEU	Marine Expeditionary Unit
MILS	Multiple Independent Level Security
MLS	Multi-Level Security
MMC	Multimedia Cards
MNLF	Moro National Liberation Front
MOE	Measure of Effectiveness
MOOTW	Military Operations Other Than War
MOP	Measure of Performance
MOS	Measure of Suitability
MUOS	Mobile User Objective System
N	
NCTAMS	Naval Computer and Telecommunications Area Master Stations
NEO	Non-combatant Evacuation Operation
NGO	Nongovernmental Organization
NIPRNET	Non-Secure Internet Protocol Router Network

NORTHCOM	Northern Command
NPS	Naval Postgraduate School
NSA	National Security Agency

O

OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OPAREA	Operational Area
OPNAV	Office of the Chief of Naval Operation
OTAR	Over-the-Air Rekey
OTAT	Over-the-Air Transfer
OTAZ	Over-the-Air Zeroize

P

PACOM	Pacific Command
PAN	Personal Area Network
PC	Personal Computer
PDR	Preliminary Design Review
PKI	Public Key Infrastructure
POT	Period of Tension
PS	Primary Suite
PVO	Private Voluntary Organization

Q

QDR	Quadrennial Defense Review

R

R2C2	Rapid Response Command and Control
RCC	Regional Combatant Commanders
RDR	Rally of Republicans (Rassemblement des Republicaines) party
RP	Republic of the Philippines
RRK	Rapid Response Kit

S

SA	Situational Assessment
SATCOM	Satellite Communication
SD	Secure Digital
SE	Systems Engineering
SEA	Systems Engineering and Analysis
SHF	Super High Frequency
SITREP	Situation Report
SIPRNET	SECRET Internet Protocol Router Network
SJFHQ-CE	Standing Joint Force Headquarters Core Element
SME	Subject Matter Expert
SOCOM	Special Operations Command

SOF	Special Operations Force
SOP	Standard Operating Procedure
SOUTHCOM	Southern Command
SSA	Situational Security and Assurance
SSH	Secure Shell
SSL	Secure Socket Layer
STEP	Standardized Tactical Entry Point

T

TACSAT	Tactical Satellite
TEMP	Test and Evaluation Master Plan
TDSI	Temasek Defense Systems Institute
TNT	Tactical Network Topologies

U

UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
UJTLs	Universal Joint Task Lists
UN	United Nations
USB	Universal Serial Bus
USJFCOM	United States Joint Forces Command; also referred to as JFCOM
USAF	United States Air Force
USN	United States Navy
USS	United States Ship

V

VoIP	Voice over IP
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VTC	Video Teleconference

W

WHO	World Health Organization

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Background

The Wayne E. Meyer Institute of Systems Engineering and the Deployable Joint Command and Control (DJC2) Joint Program Office (JPO) sponsored a Systems Engineering and Analysis Cohort Nine (SEA-9) capstone project to develop and analyze architectures for a rapidly deployable command and control system to support the Regional Combatant Commanders (RCCs) in austere environments. The U.S. military responded quickly to recent natural disasters, such as the 2004 Tsunami, Hurricane Katrina, and the Pakistan earthquakes, but lessons learned have emphasized the need for interoperable command and control systems to effectively coordinate between the military, local governments, and nongovernmental organizations (NGOs) in order to help the region(s) return to normalcy. In addition to disaster relief lessons learned, the 2006 Quadrennial Defense Review (QDR) stated the need for improved joint command and control capabilities to combat terrorism and defend the homeland.

The Rapid Response Command and Control (R2C2) integrated project team, consisting of six SEA-9 students and nine Temasek Defense Systems Institute (TDSI) students, completed a rigorous systems engineering (SE) process to address the command and control needs stated in the disaster relief lessons learned and the capability gaps outlined in the QDR. The team's problem statement was to develop and analyze architectures, and design systems for a rapidly deployable command and control system to provide RCCs with an initial situational assessment and communications capability through the range of military operations. During this process, the team conducted mission analysis, generated requirements, developed and modeled architectures, and analyzed the team-developed architectures and legacy architectures. Naval Postgraduate School (NPS) students and faculty from numerous academic and research departments, such as Information Sciences, Computer Science, Defense Analysis, Space Engineering, and Operational Research, provided additional technical and operational expertise needed to design the R2C2 system architectures.

Systems Engineering Approach

The DJC2 JPO is developing a Rapid Response Kit (RRK) "to provide state-of-the-art, agile, self-contained mobile quick response capability with a small footprint and secure access to mission critical information."[1] Other key requirements outlined in the Capability Production Document (CPD) include access of up to two data networks, such as Non-Secure Internet Protocol Router Network (NIPRNET), SECRET IPRNET (SIPRNET), and Combined ENTerprise Regional Information eXchange System (CENTRIXS), and transportable by two persons via ground, commercial, or military air. The R2C2 team reviewed all requirements in the CPD and Broad Area Announcement (BAA) to understand RRK functionality, but did not strictly use these requirements to determine the functionality of the R2C2 system. An additional top-down SE approach was conducted to generate R2C2 requirements and to evaluate the validity of the requirements for the RRK.

The process started by researching Joint Publications, the 2006 QDR, and recent peacetime and wartime operational lessons learned to determine command and control doctrine, procedures, and capability gaps. From this research, the team determined that the military needed a standardized command and control system that is: interoperable with joint, coalition, and interagency entities; modular and scalable; rapidly deployable; and maintains a small operational footprint. Once the capability gaps were identified, the team sought user guidance to determine the missions of the R2C2 and concepts of operations to help develop requirements. Due to the volume of potential users who would be receiving the system in European Command (EUCOM), Pacific Command (PACOM), Southern Command (SOUTHCOM), and Central Command (CENTCOM), and the different environments in which they operate, the team developed five different scenarios in an effort to address the broad spectrum of military operations and vetted them through the DJC2 JPO, requirements offices, and RCC representatives. The five scenarios included: 1) a humanitarian assistance operation to support Singapore during a pandemic, such as the avian influenza,; 2) a disaster relief operation to locate U.S. personnel and assist El Salvador after a devastating earthquake; 3) a

[1] DJC2, Capability Production Document, OPNAV n71C2-688(1)-71-05, 30 November 2005, p. 2.

counterterrorism operation to help the Philippine government locate a high value terrorist target; 4) a civil unrest operation in Ivory Coast to support the United Nations and conduct Non-combatant Evacuation Operations (NEO); and 5) a deployment scenario in Iran to conduct Battle Damage Assessment (BDA) and determine the staging area for a larger command and control system for continuous operations.

The five approved scenarios were developed into concepts of operations to determine the functionality of the R2C2 system. The team conducted a functional analysis from both a user's and system's perspective to determine what the system does and how the system will be used. The functions identified by the team translated into operational and system requirements and were mapped to the Chairman of the Joint Chiefs of Staff's Universal Joint Task List to ensure that the requirements traced to strategic guidance.

The operational and system requirements were used to develop multiple R2C2 architectures. By conducting market surveys for over 40 communications, sensors, information management, and power alternatives to determine technology availability and feasibility, the team reduced the selection to 8 potential architectures and 3 modular suites. The Primary, Local, and Civilian (Civil)/Military Suites allow the RCCs flexibility to operate in many different missions. The Primary Suite provides reachback to RCC headquarters and to the Global Information Grid and includes components such as routers, switches, laptops, satellite terminals, phones, encryption devices, and a generator. For architecture analysis, the team investigated alternatives for satellite terminals and determined total system weight. To provide a situational assessment of the operating area to the RCC, the Local Suite provides communications and data transfer capability within the local area and includes components such as satellite phones or military radios, cameras, personal digital assistants, and wireless networks (802.11 Wi-Fi and 802.16 Wi-Max). Modeling and analysis was used to compared data transfer rates and system weight for Local Suite architectures that included a data link and voice network versus a voice only alternative. Because humanitarian assistance and disaster relief (HA/DR) operations occur more frequently, the RCCs need to be prepared to work with their civilian counterparts and the Civil/Military Suite provides Internet access for the Civil/Military Operating Centers in the devastated region. The Civil/Military Suite

includes components such as satellite terminals, laptops, and a generator or, depending on the available bandwidth, the Civil/Military Suite could be integrated into the Primary Suite to reduce size, weight, and footprint. Modeling and analysis was used to calculate the bandwidth availability throughout the operation at the Primary Suite and to determine if enough bandwidth remained for Civil/Military Suite use. System weight with and without a dedicated Civil/Military Suite was also calculated.

Modeling the different alternatives for the Primary, Local, and Civil/Military Suite helped the team select an architecture that could best fulfill the range of military operations. The final architecture, that included a Primary Suite with a generator, a Local Suite with a data link, and an integrated Civil/Military Suite, was compared to current operational systems and a proposed system submitted by a contractor in response to the BAA. The team used multiple decision aids, including an Analytic Hierarchy Process (AHP) and a requirements stoplight comparison, to rate the different systems. The AHP utilized weighted decision criteria collected from a robust mix of academic and operational NPS users with experience in communications, information systems, logistics, networks, and tactical operations. The stoplight comparison rated each system on whether it met the requirements stated in the CPD, BAA, and the team-generated list.

Project Conclusions

The team generated additional requirements from mission analysis that were not identified in either the CPD or the BAA. The R2C2 system included organic power to ensure that constant power was available. Over 60% of the scenarios were in austere environments where the local infrastructure could not support continuous power or was devastated by natural disasters or war. In order to provide a situational assessment to the RCCs, a local communications network, to include scouts and equipment, was required to collect and pass situational reports. Since the Primary Suite was stationary, the team captured this requirement by designing a Local Suite. RCCs have responded to all the recent natural disasters and lessons learned from these operations have highlighted the need to improve coordination and cooperation between military and civilian counterparts. The team included a Civil/Military Suite to address this capability gap by providing Internet access to civilian counterparts in regions where all local and global communications have been severely damaged.

From the development and analysis of multiple models, the team selected two final Local Suite architectures. These two architectures were dependent on whether the mission was considered time-critical and a data link was required to improve data transfer rates, or if the mission was considered a normal operation and only a voice report was required. The results of the model indicated that having a voice-only link would not meet the 30-minute window between observation and action for time-critical operations. Since over 60% of the scenarios were considered time-critical, the Local Suite with a data link was used for system comparison and the R2C2 system's scout team incurs an additional 50 pounds of equipment.

The team evaluated Primary Suite bandwidth availability based on concepts of operations and varying data rates. The team modeled data rates ranging from 512 kilobits per second (kbps) to 4,096 kbps, and the results concluded that there was enough excess bandwidth (over 50%) to allow an integrated Civil/Military Suite, significantly reducing system size and weight.

The team performed additional weight trade-offs on the Primary Suite to better comply with the two-person transportable requirement. If lightweight packaging is used (vice heavy plastic cases) to transport the system, the weight can be reduced by 27 pounds, but is less robust and durable. A Norsat Globetrekker (note the use of the term Globetrekker in Chapter 5.0) satellite terminal weighs 36 pounds less than the proposed SWE-DISH system, but is not licensed on as many constellations as SWE-DISH. If the RCC determines from mission planning that the operating area has reliable power, then the generator can be left behind for a savings of 50 pounds. The combined weight trade-offs reduced the Primary Suite from 340 pounds to 227 pounds.

The results from comparing current operating systems, the proposed system, and the R2C2 system, using the AHP and the stoplight matrix decision-making tools, were consistent. Both tools identified the R2C2 system as the preferred system to perform the range of military operations. R2C2 ranked highest in the AHP at 43% compared to the current and proposed system at 29%. R2C2 also captured 27 of 28 requirements in the stoplight matrix compared to the proposed system at 22 and current system at 16. From this analysis, the team concluded that the R2C2 system delivers increased capabilities over current and proposed systems, while still meeting the requirements outlined in the

CPD and BAA, and provides the RCCs with required flexibility and scalability to deliver a rapidly deployable command and control capability to perform the range of military operations.

ACKNOWLEDGEMENT

The SEA-9 integrated project team, Rapid Response Command and Control, would like to express our thanks and sincere gratitude for the time, dedication, expertise, and guidance of the following individuals.

Dr. Frank Shoup
Dean Wayne Hughes
Dr. John Osmundson
Professor Gary Langford
Dr. Tom Huynh
Professor Karen Burke
CAPT Starr King, USN
CAPT Jeff Kline, USN (Ret.)
Mr. Michael Clement
Professor Thomas Hoivik
Dr. Michael McCauley
LTCOL Gregory Mislick, USMC (Ret.)
Dr. Patrick Parker
Dr. Robert Harney
Dr. Dave Olwell
Professor Matthew Boensel
Professor Mark Stevens
Professor Bard Mansager
Professor Doyle Daughtry
Professor Paul Sanchez
Professor William Solitario
Professor Gregory Miller

Additionally, we would like to thank the remaining faculty and staff of the Wayne E. Meyer Institute of Systems Engineering who provided direct and/or indirect support to our project and helped to ensure its success. Also, we would like to extend our thanks and appreciation to our families, whose unwavering patience, understanding, and support during long project hours was essential for our successful completion.

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 BACKGROUND OF SEA

This capstone project report and a formal presentation are requirements to earn a Masters degree in Systems Engineering and Analysis (SEA) at the Naval Postgraduate School (NPS) in Monterey, California. The report captures the key systems engineering (SE) products and design analysis used during the six-month project and provides the stakeholders with system design recommendations for the Rapid Response Command and Control (R2C2) system. The capstone project team itself was comprised of the following U.S. Navy members from SEA-9: LCDR Lisa Sullivan, LT Ronel Reyes, LT Lennard Cannon, ENS Kitan Bae, ENS Jim Colgary, and ENS Nick Minerowicz, as well as students representing the Temasek Defense Systems Institute (TDSI) from Singapore: Major Chris Leong, Major Harry Lim, Mr. Hang Sheng Lim, Ms. Chin Chin Ng, Captain Tiong Tien Neo, Mr. Guan Chye Tan, Major Yu Loon Ng, Major Eric Wong, and Mr. Heng Yue Wong. In addition to the primary team, consisting of the six SEA students as well as the nine TDSI students who have backgrounds in communications, information assurance, sensors, and operational research, students from the Information Sciences, Defense Analysis, and Computer Science Departments also contributed to the project as Subject Matter Experts (SMEs).

1.1 INTRODUCTION

The SEA curriculum, with support from the Wayne E. Meyer Institute of Systems Engineering, incorporates a capstone project that integrates the efforts of multiple disciplines at NPS and TDSI. The purposes of the capstone project are:

- To understand the concept of System of Systems
- To understand problem solving using the SE thought process
- To understand customer needs and translate them to operational requirements
- To design and develop architectures
- To model and analyze architectures

- To effectively communicate results and provide recommendations to the customer

1.2 TASKING

The current tasking statement, as outlined by the Meyer Institute and the Deployable Joint Command and Control (DJC2) Joint Program Office (JPO), is to design and analyze architectures using SE principles and products to aid in the development of a Rapid Response Kit (RRK). The R2C2 team will provide the following products to the JPO:

- Mission Analysis
- Scenarios and Concepts of Operations (CONOPS)
- Refinement of Operational and System Requirements
- Conceptual Architectures
- Models of the Architectures
- Analysis of Architectures and Recommendations

To facilitate the tasking goals, the R2C2 team has applied a systems engineering process.

1.2.1 R2C2 Problem Statement and Constraints

The problem statement for the R2C2 team was to develop and analyze architectures and design systems for a rapidly deployable, Command and Control (C2) system to provide Regional Combatant Commanders (RCCs) with initial situational awareness and communication capabilities through the range of military operations. This analysis will be provided to the DJC2 JPO to aid in the development of a RRK. To help meet the JPO's short schedule requirement to start prototyping in October 2006, the designs and architectures are predominantly commercial-off-the-shelf (COTS) products that are readily available.

1.2.2 Current Needs and Capability Gaps

The current need for R2C2, as outlined by the JPO, requires a system that can be quickly deployed into theater to facilitate C2 without requiring a large physical presence or logistic trail. The system should be flexible enough to handle most mission

requirements, while allowing for the possibility of modularity to allow for changes in functionality, as necessary.

While the JPO is aware that systems such as this presently exist throughout the U.S. military, the vast majority of them are cobbled together on an ad-hoc basis at the discretion of the commanding officer. While these ad-hoc systems likely meet the needs of the command, their interoperability and logistic support is inadequate. The JPO envisions a lightweight C2 system that can be standardized and logistically supported throughout all branches of the military to minimize the creation of multiple ad-hoc systems.

1.2.3 Relationship with DJC2 JPO

The DJC2 JPO vision is to

> . . . create a more cost-effective, superior means to deploy, furnish, install, operate, and maintain a symbiotic C2 Combat Operations Center (COC) infused with the latest advanced technology and collaboration toolsets, providing a unique capability for a Joint Task Force Headquarters or a Standing Joint Force Headquarters—allowing a Joint Force Commander to conduct JTF operations better with each spiral delivery.[2]

Therefore, the JPO initiated the creation of multiple system architectures to meet this need, depending on the level of C2 necessary. Even though this system was planned to be sizeable depending on need, it was noted that there may be several situations where the setup of even the "small" DJC2 would be infeasible.

The JPO identified a need for a smaller system that could both fulfill basic C2 operations in a standalone configuration, as well as serve as an interim C2 node if the situation warrants the setup of a DJC2 system. This RRK is envisioned to be a lightweight, man-portable system that can be transported by two personnel, operated by 4-10 personnel, and functional in-theater within days. The RRK would then be able to provide reachback and C2 functionality in a region that previously had none. The goal of this capstone project is to explore the RRK concept and provide the JPO with a series of architectures (known as R2C2) designed to meet those needs.

---

[2] Briefing given by Steve Grant, DJC2 Chief Engineer, NSWC, Panama City, FL, 21 August 2005.

1.2.4 Project Goals

To satisfy the requirements of the Meyer Institute and DJC2 JPO, R2C2 is developing the following products:

- **Mission Analysis:** To get a consistent understanding of the mission requirements for the proposed system between the system architects (R2C2) and the primary stakeholders (DJC2 JPO), a series of missions and scenarios were developed to highlight what the R2C2 team determined to be key attributes of the system. These missions were then presented to the stakeholder for review and input. Once the stakeholder and designers both agreed that the proposed missions indicated a need for an R2C2 architecture due to a capability gap, the missions were detailed out into specific scenarios.
- **Scenarios and CONOPS:** Starting with the proposed missions for the R2C2 system, the R2C2 team then further decomposed the missions into specific scenarios, as well as laid out the preliminary CONOPS necessary for the employment of the system architecture.
- **Refined Operational and System Requirements:** Through communications with the DJC2 JPO, SMEs, and RCC representatives, as well as analysis of team-developed scenarios, a series of operational technical requirements were created to help guide the creation of system architectures.
- **Conceptual Architectures:** Once there was a consistent understanding about what the requirements are for the system, system architecture alternatives and variants were designed to fulfill the developed operational requirements. These architectures were then modeled and evaluated for effectiveness.
- **Models of the Architectures:** As the different architectures for the system were developed, executable or numeric models were created to assess and estimate the performance of the proposed alternatives. Additionally, models of missions and scenarios were used to more closely evaluate the system from an "operational" perspective.

- **Analysis of Architectures and Recommendations:** Once the models of the design architectures were complete, the results were analyzed to determine how they relate to each other in terms of overall performance. Key conclusions and recommendations will be presented to DJC2 JPO and forwarded to the RCCs.

1.2.5 Important Dates

The duration of the R2C2 project was approximately five months beginning in January 2006. This is in line with the DJC2 JPO's schedule, which requires that the SE effort of this capstone project be completed by September 2006. The R2C2 project has had three reviews, as well as a paper and final presentation. The dates for each major phase of this capstone project are listed below:

- **Conceptual Design Review (CoDR) (2/06/06):** The CoDR presented the initial capstone project's research to NPS faculty for critique and dscussion. At this phase, the R2C2 team had a solid understanding of the tasking statement and determined the project's direction and scope. This included an early understanding of operational requirements, as primarily outlined through developed scenarios discussed with the JPO.
- **Preliminary Design Review (PDR) (3/21/06):** During the PDR, the R2C2 team presented refined mission and scenarios and functional analysis diagrams to highlight some of the critical requirements and aspects of the R2C2 system. The team covered proposed architecture designs, as well as preliminary methods of comparison to analyze architectures.
- **Critical Design Review (CDR) (5/01/06):** The CDR was the third major capstone project review. By this point, the R2C2 team had fully determined system architectures as well as developed methods or models to analyze the proposed architectures. Modeling and analysis results were presented to the DJC2 JPO and NPS faculty.

- **Paper Draft Due to Editor (5/08/06):** The final paper was submitted to the editor approximately one month before graduation to allow for a proper amount to time to edit and format the document to NPS standards.
- **Final Presentation (6/05/06):** Prior to graduation, the R2C2 team briefed the integrated capstone project to the DJC2 JPO and NPS faculty. This cumulative brief included highlights of the previous three design reviews as well as any final analysis that occurred after the CDR.

1.3 SYSTEMS ENGINEERING (SE) METHODOLOGY

The SE approach to architecture design is a modern method of analyzing the management and engineering practices necessary to produce positive results by giving the development process a consistent structure or methodology.

1.3.1 What is SE and Why is it Important?

SE is a discipline that seeks to look at the system as a whole and lead the design process toward a product that meets the qualities and requirements desired by the customer. In general, SE is a practical approach to organizing both the technical and managerial aspects normally associated with a project. Following a well-defined SE process helps ensure that a project meets essential requirements and milestones as it moves toward completion.

1.3.2 SE Approaches

The SE process has several well-known examples. One such example is the "Waterfall Model."[3] It is a series of steps starting at requirements analysis and ending at system support. As the project "falls" down the waterfall, each step brings it closer to completion. The "Spiral Model"[4] is a different approach that breaks the SE process into a long series of smaller increments. Each "revolution" around the spiral is then iteratively checked to ensure that work does not proceed until known risks have been mitigated.

---

[3] Kevin Forsberg and Hal Mooz, *Visualizing Project Management*, 3rd ed., Hoboken, NJ: John Wiley & Sons, 2005, pp. 104-106.

[4] Ibid., pp. 107-108.

Both approaches focus on the entire life-cycle of actual systems. A modified SE approach that used aspects of both the "Waterfall Model" and the "Spiral Model" was developed to fit the needs of our capstone project.

1.3.3 Our Process

The R2C2 team developed a modified SE approach that included a series of steps, like the "Waterfall," to allow movement from phase to phase, and feedback loops to encourage product refinement based on stakeholders' inputs. The major phases include Research, Conceptual Design, Preliminary Design, and Design Evaluation as seen in Figure 1.

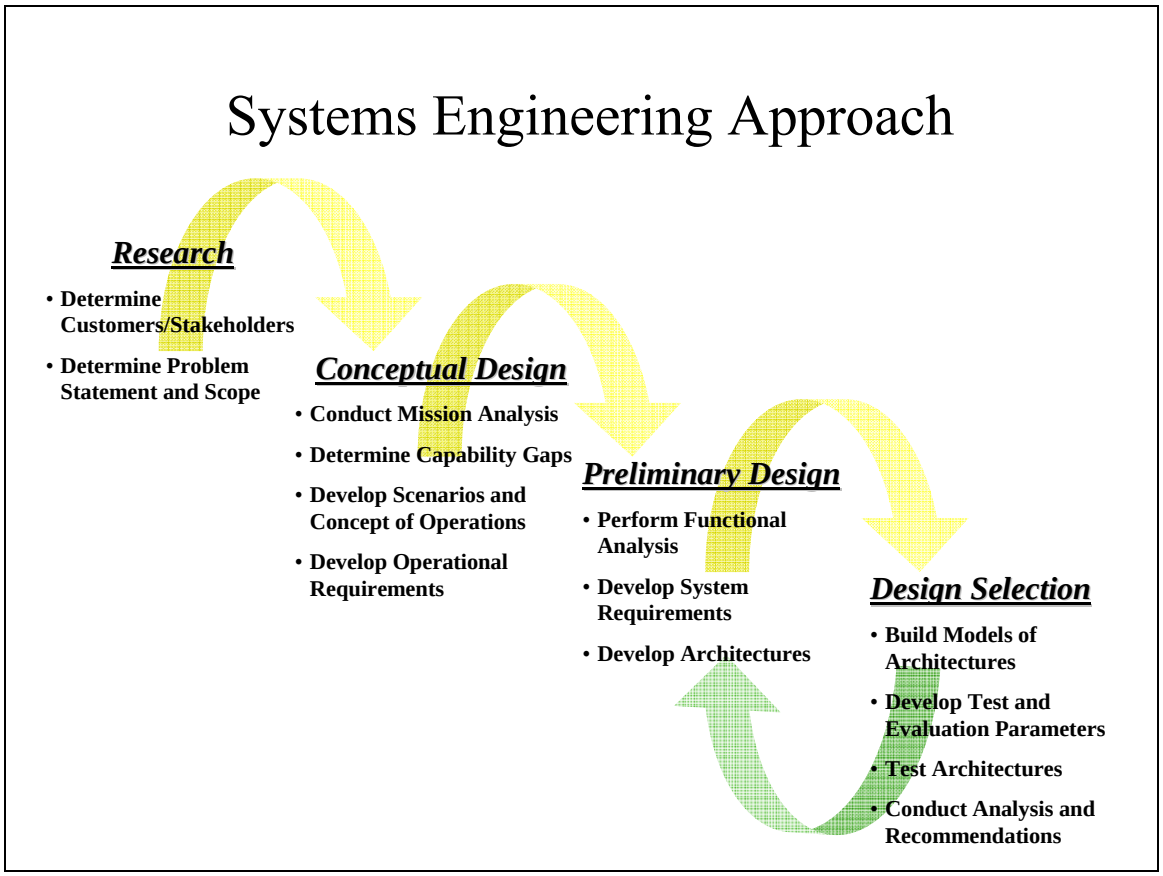


Figure 1: Systems Engineering Approach

1.3.3.1 Research

- **Determine Customers and Stakeholders:** The first step in the process was to find which entities may have an interest in the proposed capstone

project. These stakeholders were able to provide valuable input and direction for the R2C2 team.

- **Discuss with the Customers and Stakeholders:** The problem statement was discussed with the relevant stakeholders to get an understanding of their view of the problem. As the capstone project research is largely academic in nature, an emphasis was placed on how the SE process can be used to explore the problems of the stakeholder.
- **Determine Problem and Scope:** Before proceeding to system design, the R2C2 team first examined the full breadth of the possible topics and the depth of research conducted. At this point, the team determined what portion of the "overall" problem could be accomplished in the given time frame.

1.3.3.2 Conceptual Design

- **Conduct Mission Analysis:** Once the problem statement was well defined, a series of proposed missions was developed to analyze the manners in which the system may be employed. These missions helped to ensure that the R2C2 team and stakeholders had a similar vision for the system.
- **Determine Capability Gaps:** After analyzing the missions and environments in which the system must operate, the R2C2 team determined capability gaps between preliminary architectures (or existing systems) and the proposed mission profiles.
- **Develop Scenarios and CONOPS:** Once the mission analysis was complete, a more detailed set of scenarios was developed to highlight the manners in which the system will be used. The R2C2 team then checked with relevant stakeholders to ensure that the group's vision for the system was consistent with the stakeholders' requirements.
- **Develop Operational Requirements:** After developing the mission scenarios, the R2C2 team determined operational requirements for system (and mission) success.

1.3.3.3 Preliminary Design

- **Perform Functional Analysis:** Knowing the operational requirements for the system, it was then possible to perform a functional analysis on the design. This analysis is important to the SE process because it determines system interactions (i.e., people, hardware, and software), helps define requirements, and provides necessary feedback to improve scenarios.
- **Develop System Requirements:** Drawing on the results of the functional analysis, as well as any customer input, the R2C2 team determined the detailed system requirements that must be present in all of the design alternatives.
- **Develop Architectures:** With the system requirements fully explored, the R2C2 team designed several systems to fulfill those needs. While each system may not necessarily be similar in design or mission capability, they were all evaluated against each other using stochastic or executable models.

1.3.3.4 Design Evaluation

- **Build Models:** Once architectures were designed to meet the system requirements, software models were developed to evaluate the different design alternatives against each other or existing systems.
- **Develop Test and Evaluation Parameters:** Concurrent to the development of models was the creation of test and evaluation parameters. As important test criteria were identified, they were integrated into developed models and simulations.
- **Test Architectures:** Once the architectures and test criteria were finalized, the developed models and simulation were used to evaluate the level of performance for each alternative.
- **Conduct Analysis and Recommendations:** The results of the testing and evaluation phase were then analyzed to determine the effectiveness of each architecture design. Based on this analysis, the R2C2 team will provide recommendations to the JPO.

1.3.3.5 Project Organization

Project personnel were organized into the working groups displayed in Figure 2:

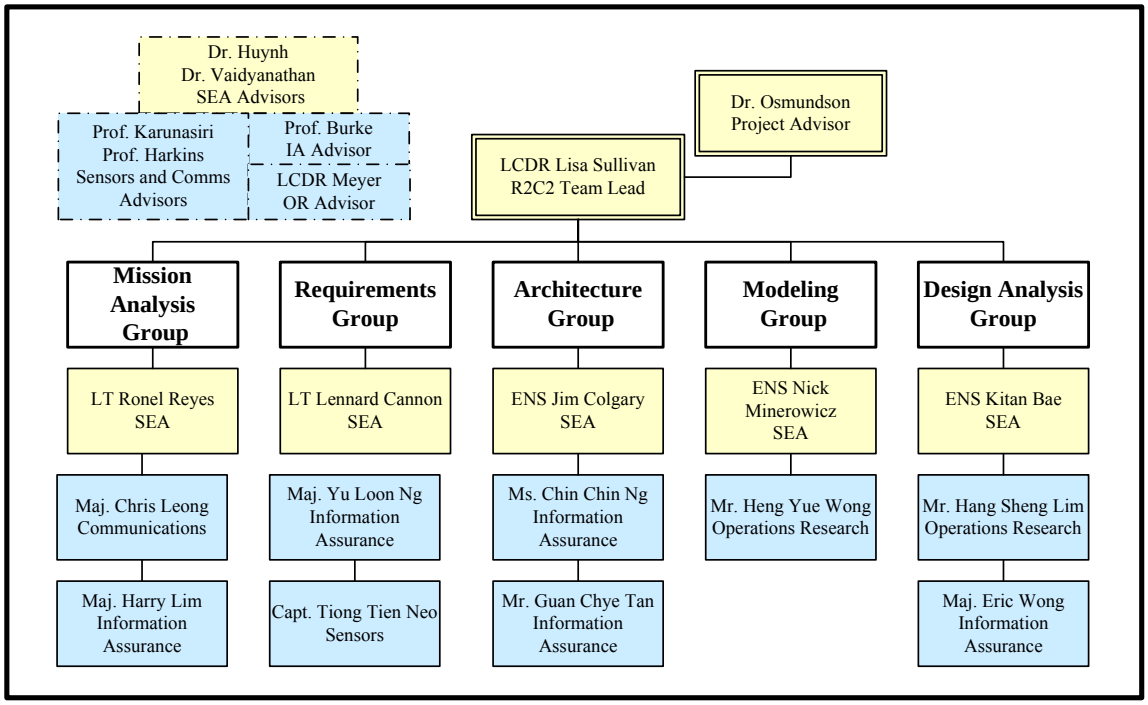


Figure 2: R2C2 Organizational Chart

Each member of the NPS SEA program was given a "group lead" position for essential elements of the R2C2 design effort. The specifics for each position are as follows:

- **Team Lead**: The project's Chief Systems Engineer; plans, organizes, and manages team functions and provides an interface between the project team and outside entities. Responsible for quality assurance of team products.
- **Mission Analysis**: Responsible for leading the group in conducting mission analysis and developing scenarios, CONOPS, and scenario timelines.
- **Requirements**: Responsible for leading the group in developing a functional analysis to determine operational and system requirements based on mission analysis and scenario development.

- **Architecture**: Responsible for leading the group in researching and developing architectures and processes necessary to design the system.
- **Modeling**: Oversees the development of system modeling efforts and is responsible for coordinating with the Requirement group to ensure that the models measure desired system requirements.
- **Test and Evaluation**: Manages and organizes the overall process of Test and Evaluation of the conceptual architectures including development of Measures of Effectiveness (MOE) and Measures of Performance (MOP).
- **Configuration Management**: The configuration management role is an additional duty assigned to the Design Analysis group and they will ensure the integrity of project files and records, as well as taking an active role in the creation and editing of new project documentation.
- **Advisors**: The project advisor will guide and assist project members in order to keep project efforts working toward project and educational goals.
- **SMEs**: While not explicitly members of the R2C2 team, SMEs may be used as consultants in specific fields.

Each working group was responsible for leading the R2C2 team during their phase of the project. All R2C2 team members were required to participate in every phase to ensure a consistent project vision.

THIS PAGE INTENTIONALLY LEFT BLANK

2.0 MISSION ANALYSIS

2.1 INTRODUCTION

The next phase completed in the R2C2 team's SE process was the mission analysis, which encompassed multiple iterative steps in order to reach the objective of implementing the system into a range of scenarios. First, to fully grasp the potential of the R2C2, an understanding of what an R2C2 is, along with what it is tasked to do was needed. As a group, the R2C2 team had limited experience with C2 doctrine, equipment, and application. With only a general knowledge of C2, the intricacies of an effective and efficient system needed to be explored.

The need for the R2C2 was researched to gain a deeper understanding of what a C2 system entails. Documents provided by the DJC2 JPO included requirements for the RRK, which gave a basis for searching for a system need. The R2C2 team was faced with defining the reason or need for such requirements. Derivation of a need for the R2C2 led to the research and identification of capability gaps between the R2C2 and current C2 systems employed by the military. These gaps provided a foundation for requirements development and refinement more thoroughly discussed in Chapter 3.0.

To further clarify the use of the R2C2, the end users of the system had to be identified. Ultimately, the RCCs represented the stakeholders of the system. Along with having many RCCs as users, the number of region-specific missions had to be investigated. For analytical purposes, determining the mission types and different scenarios that would meet these missions was the next challenge. Developing five scenarios that catered to the number of users and environments displayed the capability of the R2C2 to operate in a wide spectrum of missions.

Finally, these scenarios were sent out to our stakeholders for feedback to determine the realism of the missions depicted. As part of the SE process, input from the customer was critical and proved to be essential in updating the scenarios and reducing the scope of R2C2 operations. Confirmation of the validity of the scenarios by representatives from the requirements offices, RCCs, and the JPO helped to complete task of mission analysis.

2.1.1 Characteristics of an R2C2

The approach to define the R2C2 system requirement was to articulate the demands and limitations from each system perspective, in the context of R2C2, and address their interdependencies. We defined these system perspectives broadly as: User, Mission, Environment, and Technology perspectives. A fifth perspective of (budgetary) Resource, as well as the related lifecycle management, was investigated for the purpose of this project. Figure 3 visually depicts the relationship between the five perspectives. The intent of this approach was to provide a balanced perspective during the front-end developmental phases of the project, capturing all the proper future requirements.

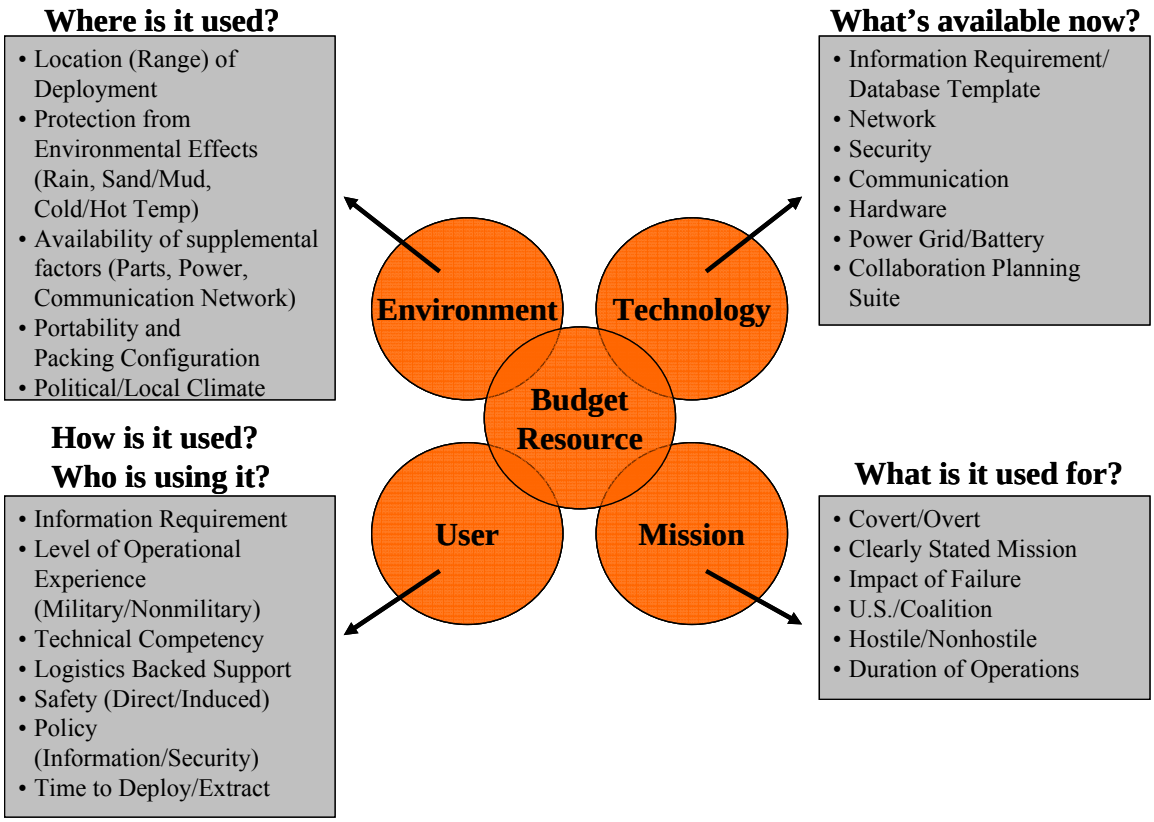


Figure 3: Characteristics of an R2C2

2.1.2 User Perspective

The user perspective would be segregated into two broad categories, namely the system owner and the system operator. The R2C2 system stems from a need to bridge information capability gaps, as determined by the system owner. These capability gaps formed the basis of the system owner perspective. The system owner had articulated the

capability gap as information requirement. In order for exchanges of meaningful information, the attributes and conduit of the information had to be defined. In addition, the system owner needed to define the information security policies that could be implemented to mitigate the risk associated with the exchanges of information. The system owner had the social responsibility to ensure that the system would not cause harm to the operators and the environment in the course of operation. The design of the system had to take into consideration the quantity and relevant operational and technical experience of the operator. This would subsequently affect the logistics support concept for the system. The classification of the operator (military or nonmilitary and level of security clearance) would similarly impact the design considerations. Well-designed interfaces between the system and the operator greatly enhance the effectiveness and efficiency of the operator in deployment.

2.1.3 Mission Perspective

The developer had to understand the covertness and hostility of potential operations. In addition, the nature of the operation, be it U.S. Department of Defense (DoD), U.S. Government, or Coalition, would impact the solution for physical and information security. The clarity of the mission's objectives (explicitly stated objectives or sense and response objectives) would determine the decision support system requirement. System risk management included the frequency of system failure and the impact of system failure for analysis. The logistics support required to sustain the R2C2's mission would be greatly determined by the duration of the operation.

2.1.4 Environmental Perspective

The developers also had to understand the location of the deployment in order to determine the environmental factors. With this knowledge, they could design the necessary protection against the effect of these environmental factors (e.g., rain, sand, dust, mud, snow, and extreme temperatures). The environment might offer dependable solutions to the infrastructure and logistics support issues, e.g., replacement parts and accessories, power supply and communication network, and the local political and social

climate. The trafficability of the environment would dictate the portability and packing configuration (shock and water proof), with consideration of the physical carrying limits.

2.1.5 Technology Perspective

The project strategically employed existing technology to bridge the capability gaps. Given the constraint of existing technology, the R2C2 team addressed two key issues, namely:

- What would be the technology requirements?
- What would be the technology available for deployment?

The information requirement would need some form of database (DB) to contain the data. A DB template would be required to define the attribute of the information and information management suite would be needed to facilitate the operator to receive, store, process, and transmit information. This suite, in addition to other physical security mechanisms, had to implement the necessary security policies. The conduit for information transfer depended on the availability of communication means vis-à-vis the frequency and bandwidth requirement. The user determined if the site dependent communication network (e.g., Global System for Mobile (GSM) Communication, Wi-Fi (IEEE 802.11), Wi-Max (IEEE 802.16)) was adequate or if a nonsite-dependent communication network (e.g., satellite communication such as Iridium phones or SATCOM radios) was necessary. The network topology and footprint would determine the type of technology or protocol required. The amalgamation of the above requirements translated to hardware requirements in terms of battery and power as well as the size of storage and speed of the processor. An R2C2 team market survey was conducted on COTS technology to determine the current state of technology for immediate implementation.

2.2 RESEARCH PHASE

To begin the capstone project, the team developed many questions to determine the purpose and functions of an R2C2. The most important questions that the team had to address early were: why do we need an R2C2 and does a capability gap exist? To answer these questions, the R2C2 team researched multiple articles from recent military

operations, military doctrinal and policy documents, and DJC2 JPO documents; interviewed SMEs and stakeholders; and observed on-going C2 exercises and demonstrations at NPS. Journal articles, magazines, TV reports, and recent military documents provided many C2 lessons learned from the 2004 Boxing Day Tsunami and Hurricane Katrina of 2005. The Quadrennial Defense Review (QDR) 2006 and Joint Publications captured strategic and operational C2 recommendations. To understand C2 concerns at the tactical level, the team interviewed stakeholders; SMEs in operations, networks, and communications; and NPS faculty and students who developed rapidly deployable Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR). The R2C2 team observed Tactical Network Topologies (TNT) and Coalition Operating Area Surveillance and Targeting System (COASTS) exercises to learn about new technology and their limitations when employed. Documents from the DJC2 JPO, such as the Capability Production Document (CPD) and the Broad Area Announcement (BAA), provided background and requirements for the DJC2 systems and initial requirements for the RRK.

2.2.1 Lessons Learned

The type of scenario, whether it is peacetime, tension, or war, dictates how the U.S. military, foreign forces, regional and international organizations (IOs), and nongovernmental (NGOs) and private voluntary organizations (PVOs) organize and collaborate. Recent peacetime operations, such as HA/DR, have presented more of a challenge for the military because each are distinctive and require interaction with so many different organizations. The military has many capabilities or "means" to offer during peacetime crisis response scenarios including C2, intelligence, planning, training, and logistics support, but are limited in the "ways" to accomplish the mission because they are not established within the crisis country or region.

2.2.1.1 Boxing Day Tsunami and Hurricane Katrina

Many reports circulated about the lack of interoperability between the military, local governments, IOs, and NGOs after the Boxing Day Tsunami in 2004 and Hurricane Katrina in 2005. First responders faced technical problems when trying to

communicate due to the different types of radios, frequencies, and/or cell phone systems being utilized. Different communication standards were not just a problem between the military and other organizations. During Katrina, Louisiana parishes quickly discovered that local and state government personnel, including police, firefighters, and medical personnel, were communicating on separate radio systems and frequencies. In addition to interoperable communications systems, both natural disasters lost critical infrastructure, such as power and communication towers, that compounded the problem and slowed relief efforts. Local officials attempted to use satellite phones to coordinate relief efforts during Katrina, but the batteries quickly died and power was unavailable to recharge.[5]

Organizational problems and policy requirements also reduced the C2 capabilities for relief operations. Nevertheless, USS ABRAHAM LINCOLN quickly arrived to provide assistance after the Tsunami, although the proper links between military and nonmilitary agencies had not been established to allow the military to seamlessly conduct relief operations. The United Nations (UN)-NGO compound was ten miles from the military operations center at the airfield making it difficult to coordinate between organizations.[6] There were limited attempts to establish a Civil-Military Operations Center (CMOC) and the military chose not to move from the airfield to the already established UN-NGO compound. Because they did not share the same workspace, military and nonmilitary organizations did not go out of their way to share information. CDR Eric Rasmussen, MC, USN, observed the following during the Tsunami relief effort:

> Aboard the carrier USS Abraham Lincoln a team member and I attended the evening Flag Brief. The information presented in the brief was extremely valuable and, in part, was unclassified. The evening Flag Brief as an event, however, was classified Secret and so could not be attended by the thirty or so members of the United Nations-U.S. Agency for International Development-NGO Interagency Assessment Team that had flown aboard that afternoon.[7]

---

[5] David Perea, "Missed Signals," *Government Executive*, February 2006, pp. 53-56.

[6] Eric Rasmussen, CDR, MC, USN, Report on "Assessing Information Support at the Civil-Military Boundary, Operation Unified Assistance in Indonesia," 6-17 January 2005, p. 8.

[7] Ibid., p. 9.

The briefs contained security reports and local images that were critical to all organizations involved, but were not shared.

2.2.1.2 Recommendations for HA/DR Operations

Many articles and documents recommended early identification of interoperability problems through exercises and training in order to improve the effectiveness of HA/DR operations. Response organizations, such as the military, need to address the hard science of hardware and software system interoperability and organic power alternatives and the soft science of developing relationships with other organizations to improve collaboration. Conducting planning and exercises that focus on interagency and military cooperation are important to improving response time and building trust.

> Finally, we must continue to emphasize that our senior officials routinely participate in rehearsals, gaming, exercises, and simulations, as well as the Contingency Planning Interagency Working Group which has become a genuine leap forward in the effort to establish a sound system to incorporate crisis and deliberate planning across the interagency.[8]

The Strong Angel exercise, held periodically in San Diego, includes the San Diego Emergency Operations Centers, city police, Emergency Medical Service (EMS), hospitals, medical directors, churches, radio stations, airports, Federal Bureau of Investigation (FBI), and military participants to address disaster relief. The focus of the exercise in August 2006 will be on establishing communication links between the various players to increase situational awareness for a pandemic scenario. All organizations participate in planning and execution to determine current capability gaps in technology, policy, and organizational structure.[9]

---

[8] Joint Chiefs of Staff, Joint Warfare of the Armed Forces of the United States, Joint Pub 1 (Washington, D.C.: 14 November 2000), VI-5, Chairman of the Joint Chiefs of Staff (CJCS) Posture Statement before the 106th Congress Committee, On Armed Service, United States Senate, 8 February 2000.

[9] Strong Angel III, San Diego, CA from 20-26 August 2006, Overview, Hosting Requirements, and Task List, 16 January 2006.

2.2.2 QDR 2006

The QDR 2006 captured current military missions and identified future missions that require new or improved capabilities. The DoD shifted its focus from preparing for a single, predictable threat to planning for multiple irregular, asymmetric operations to support the Global War on Terror (GWOT).[10] Recent wartime operations, such as Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), and HA/DR efforts, such as the Boxing Day Tsunami, Hurricane Katrina, and the Philippine Mudslides, have introduced new challenges for the U.S. military and their ability to quickly and effectively respond. The QDR emphasized the need for improved Joint C2 and Net-Centricity capabilities to defeat terrorist networks and defend the homeland in depth.

2.2.2.1 Defeating Terrorist Networks and Defending the Homeland in Depth

To address the new strategic and operational challenges of GWOT and homeland defense, the U.S. military must cooperate and integrate with other services, government agencies, and coalition partners. Many policies do not allow organizations to share time-critical information, limiting mission effectiveness. In addition, the majority of systems are not interoperable, causing communication challenges. The QDR identified that

> . . . the Department seeks to improve the homeland defense and consequence management capabilities of its national and international partners and to improve the Department's capabilities by sharing information, expertise and technology as appropriate across military and civilian boundaries.[11]

Recent events, involving U.S. troops, have covered the spectrum of military operations and have demonstrated the need to work with multiple organizations. The QDR highlighted the need for Joint C2 to:

- **Defeat Terrorist Networks:** Joint coordination, procedures, systems, and when necessary, C2 to plan and conduct complex interagency operations.

---

[10] *Quadrennial Defense Review*, 6 February 2006, p. vii.

[11] *Quadrennial Defense Review*, 6 February 2006, p. 29.

- **Defend the Homeland in Depth:** Joint C2 for homeland defense and civil support missions, including communications and C2 systems that are interoperable with other agencies and state and local government.[12]

2.2.2.2 Joint C2

In addition to identifying a need for interoperable hardware and software for C2 and communication systems, the military has emphasized the importance of organizing and training C2 personnel to improve mission effectiveness. The Standing Joint Task Force Headquarters Core Element (SJFHQ-CE) has recently been developed to rapidly deploy and provide Combatant Commanders with additional trained personnel to plan and execute crisis action operations with other agencies and coalition partners. SJFHQ-CEs are standing, coherent teams of "joint generalists" led by a flag or general officer. They are full-time, Joint C2 elements within the RCC's staff. They are mission-tailorable and bring extensive knowledge of joint operations, the area of responsibility and its key issues and regional players, as well as an on-going understanding of the RCC's theater perspective to the Joint Task Force (JTF).[13] The SJFHQ-CE also supports the DoD's vision of Net-Centricity to accelerate the decision-making process by harnessing the power of information connectivity by enabling critical relationships between organizations and people.[14] The metrics that will determine SJFHQ-CE effectiveness are 1) the reliability of communications and information systems and 2) the ability to coordinate and foster trust among other organizations in the early stages of crisis response.

2.2.3 Joint Publications

To gain an understanding of how the military currently plans and operates for different missions and environments, the R2C2 team researched multiple Joint Tactics, Techniques, and Procedures (JTTP) documents. These documents described the current U.S. military policy and doctrine based on lessons learned from previous operations.

---

[12] *Quadrennial Defense Review*, 6 February 2006, p. 27.

[13] United States Joint Forces Command, "Standing Joint Force Headquarters Core Element," http://www.jfcom.mil/about/fact_sjfhq.htm, 18 January 2006.

[14] Ibid., p. 58.

They also gave insight to challenges, capability gaps, and manning requirements associated with each mission. The Joint Publications (JP) researched included: Joint Warfare of the Armed Forces of the United States (JP 1), Doctrine for Joint Operations (JP 3), Doctrine for Joint Special Operations (JP 3-05), JTTP for Noncombatant Evacuation Operations (JP 3-07.5), and Interagency Coordination During Joint Operations, Vol. I, (JP 3-08). The Joint Doctrine for Military Operations Other Than War (MOOTW) (JP 3-07), 16 June 1995, and Joint Communications Systems (JP-06), 20 March 2006, specifically addressed our capstone project and are discussed below.

2.2.3.1 Joint Doctrine for MOOTW (JP 3-07)

JP 3-07 defined MOOTW as "the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war." JP 3-07 provided insight to the many considerations required for multinational operations including: set common goals, support unity of effort, improve national force through training and share common resources, learn and respect cultural differences, and ensure communication capability to respective coalition leaderships.[15] The specific missions of MOOTW are discussed in depth later in this chapter.

2.2.3.2 Joint Communications Systems (JP 6-0)

In addition to defining current communication systems and terms, the JP 6-0 helped the R2C2 team determine, "who needs to exchange info with who." For planning and management, the JP 6-0 identified the need for modular packaging, interoperability, standardization, and commercial capabilities. Since military operations rarely occur in the same location, the RCC should plan for the communications system to be built-up incrementally and with modular capability to address the specific mission needs. Including common and standardized equipment can mitigate the risk of

[15] United States Joint Chiefs of Staff, *Joint Doctrine for Military Operations Other Than War*, Joint Pub 3-07, Washington, D.C.: 19 June 1995, p. IV-4.

noninteroperable systems. Commercial systems can ease logistic and training problems due to their availability and use worldwide, thereby reducing the amount of equipment needing to be transported into theater.[16]

2.2.4 Interviews

The team conducted multiple interviews to determine potential stakeholders and system users, analyze current operational C2 issues, develop a problem statement, and determine project scope. NPS faculty, students, and technical representatives provided insight into current operations and available technology. The SMEs included U.S. Navy Special Warfare Officers, information professionals, and U.S. Marine Corps Communications Officers. Their experience and expertise helped the team develop realistic scenarios and architectures. NPS faculty from the Systems Engineering, Operations Research, Defense Analysis, Naval War College, Space Engineering, and Information Sciences Departments provided potential contact information and feedback on the proposed scenarios. Multiple interviews with the primary stakeholder, DJC2 JPO, supplied the background of the DJC2 system, determined RRK mission and user requirements, and provided feedback on the SE products developed by the R2C2 team. Representatives from CENTCOM, Joint Forces Command (JFCOM), Air Force Contingency Response Group, and Net-Centric Warfare Division (N71) also submitted feedback on the generated scenarios.

2.2.5 Current NPS C2 Efforts

There were many on-going C2 theses, projects, and exercises that the team investigated to gain test and evaluation insight and ideas for potential R2C2 architectures. HFN, COASTS, and TNT utilized COTS and emerging military technologies to develop C2 architectures and tested them in varying environments. From their input, the R2C2 team gathered valuable metrics for communications, such as range, bandwidth (BW), power, and system integration, in an operational environment to supplement component specifications given by commercial companies or open sources.

---

[16] United States Joint Chiefs of Staff, *Joint Communications System*, Joint Pub 6-0, Washington, D.C.: 20 March 2006, pp. III-18 - III-20.

2.2.5.1 COASTS and HFN

The coalition-based research program, COASTS, was "a field experimentation program designed to research low-cost, state-of-the-art, rapidly scaleable airborne and ground communications suites including various wireless network technologies."[17] COASTS students, faculty, and contractors have conducted multiple peacekeeping and law enforcement exercises with the Royal Thai Armed Forces in Thailand to demonstrate C2 technologies and foster coalition relationships. COAST explored field experimentation research in: wireless network technologies, ultra wide band technologies, GPS tracking, sensors, wearable computing devices, unmanned aerial vehicles (UAV), situational awareness applications, persistent surveillance, and foreign language translation devices.

The HFN group included personnel and equipment involved with the COASTS program, but they focused on HA/DR response. After the Boxing Day Tsunami, the HFN group quickly deployed to the devastated region to set-up Internet connectivity at a survivor camp and a graves registration center.[18] Networks were established in five days and remained operational for five months.

> Users immediately took advantage of their newfound Internet connectivity. NGO's and IO's found it convenient to communicate with the home office, media personnel were in direct contact with their colleagues and family members or friends of the hundreds of missing relatives/friends were able to send and receive pictures of those they were looking for.[19]

Shortly after returning from Thailand, the HFN group deployed to Bay Saint Louis, Mississippi to provide Internet connectivity to local government departments. From experiences learned in HA/DR, HFN students and faculty have improved FLy-Away-Kit (FLAK) prototypes to provide rapidly deployable network nodes. The R2C2 team included FLAK concepts when evaluating current designs and analyzed its capability in Chapter 6.0.

---

[17] Coalition Operating Area Surveillance and Targeting System 2006 Overview.

[18] Report on Naval Postgraduate School response to the 2004 Southeast Asian Tsunami, "Hastily Formed Networks for Complex Humanitarian Disasters and Emergencies," 25 July 2005, p. 3.

[19] Ibid., p. 10.

2.2.5.2 TNT

TNT conducted quarterly exercises to demonstrate new technologies to support the near term needs of the warfighter. NPS students and faculty, the Special Operations Command (SOCOM) Advanced Technology Directorate, industry partners, and national laboratories participated in these exercises to identify "key gaps and deficiencies resulting from applications of advanced technology, particularly network communications, unmanned systems, and net-centric applications."[20] The R2C2 team observed experiments at Camp Roberts, California that involved: high bandwidth communications for urban operations, convoy tracking using a controlled UAV, field biometrics, and field information analysis and collaboration.

2.2.6 DJC2 Documents

The DJC2 JPO submitted a CPD in November 2005 for the Milestone C Decision.[21] The CPD provided the R2C2 team with background information on the DJC2 program and requirements for En Route, Early Entry, and Core systems. All DJC2 systems have similar functions, but are different in scale. The En Route system supports a small C2 capability for 10-20 operator positions, while en route to a deployment site. The Early Entry system supports 20-40 operators and the Core system scales up to support a JTF of 60 operator positions. To address the RCCs' need for an even smaller system to rapidly deploy for crisis action response, the RRK was augmented as a new requirement into the CPD to

> . . . provide a state-of-the-art, agile, self-contained mobile, quick response capability with a small footprint; with secure access to mission critical information and support staff using satellite connectivity designed to serve up to four operators, expandable up to ten in group collaboration with reachback and is readily transportable on commercial or military aircraft.[22]

The CPD contains initial RRK system requirements, but does not explain the type of missions or tasking that the system will perform.

---

[20] TNT Overview Report, 2006.

[21] Milestone C is a DoD decision review used to evaluate products completed during the system development and demonstration phase and is required before starting the production and deployment phase.

[22] DJC2, CPD, OPNAV N71C2-688(1)-71-05, 30 November 2005, p. 8.

Shortly after the CPD was released, the DJC2 JPO prepared a BAA for companies to submit proposals for the RRK. The BAA included the technical parameters that the proposed systems must meet or exceed. Some of the technical parameters cited in the BAA are not required in the CPD, which caused confusion for the JPO and the R2C2 team. The differences in the two documents, and how the R2C2 refined the requirements, are explained in Chapter 3.0.

2.3 NEEDS ANALYSIS AND CAPABILITY GAPS

The need for a system such as the R2C2 has evolved as the military takes on an increased role in assisting countries in crisis action response or HA/DR operations. As the military continues to become faster and lighter, it needs a rapidly deployable system that can conduct a wide range of missions from peacetime operations to full-scale war. The RCCs are tasked to deal with these issues as they arise, which is why, "The 2006 QDR provides new direction for accelerating the transformation of the Department to focus more on the needs of Combatant Commanders."[23] This shift in focus generated the need for a standardized C2 collaborative system and construction of ad hoc C2 systems were no longer an acceptable practice. Thus, the DJC2 JPO came into existence with the goal of developing a system that provides a seamless, shared information environment supporting Joint, Multinational, and Interagency operations.[24]

Initial conceptual design of the DJC2 included three configurations of the scalable system: En Route, Early Entry, and Core configurations. Each configuration can be thought of as a different phase in the system. The configurations increased in size, beginning with En Route and ending with the Core, and each was capable of being a stand alone C2 system. After the JPO held a user's feedback session with representatives from the RCCs, the requirement for a smaller system was proposed by EUCOM. This proposal resulted in the RRK being supplemented into the CPD.

Although EUCOM had expressed the want for a smaller C2 system, the R2C2 team's SE approach further explored the customer's actual need for such a system.

---

[23] United States Department of Defense, *Quadrennial Defense Review*, 2006-04-17, p. 3.

[24] DJC2, CPD, OPNAV, N71C2- 688(1)-71-05, 30 November 2005, p. 2.

As a starting point for identifying a need, the requirements for the RRK were looked into. The R2C2 team researched the generation of requirements found within the DJC2 CPD and the RRK BAA to help define the need. Correspondence was done with the Office of the Chief of Naval Operations (OPNAV) N71C2, United States Joint Forces Command (USJFCOM) J88, and DJC2 JPOs to determine the basis for the outlined requirements. It was discovered that user inputs from the RCCs drove the requirements generation.

For additional insight, interviews and discussions were held between the R2C2 team and SMEs across the NPS campus. These SMEs included service members in the Special Operations community, military faculty members with experience on the strategic, operational, and tactical levels in a Joint environment, and civilian faculty members with similar experience or background. They were asked to discuss some of their operational experiences, the type of equipment they used, what equipment was lacking, if any, and could an R2C2 help them out. From these talks, an asset such as the R2C2 proved to be a much needed system to have for the range of operations the military encounters. It was mentioned repeatedly that an R2C2 would have either made the mission easier or improved their capability.

From their research and analysis, the R2C2 team identified a needs statement for the R2C2. The statement was deduced to be: The RCCs need a deployable, standardized C2 system with a small footprint to be utilized by first responders in Joint, Civil-Military, and Coalition operations.

Next, the capability gaps produced by the introduction of an R2C2 system were studied. RCCs have existing systems that have similar functions to the R2C2 system; however, they were not standardized or interoperable across services or RCCs. Current systems employed by the U.S. military were researched and a detailed comparison was done between the capabilities offered by current systems and the capabilities of the R2C2. This involved analysis of not only the system capabilities of various equipment, but also the tactical employment and doctrine behind the use of the equipment.

The R2C2 team discovered that the RCCs do not have standardized, common, interoperable, and rapidly deployable C2 capability to support Joint, Multinational, and Interagency Operations. As mentioned earlier, ad hoc systems were commonplace for RCCs to implement when deploying C2 systems. For instance, a particular RCC may use

one type of arrangement of equipment different than another RCC to do the same mission. They also lack the modular and reconfigurable design to permit flexible addition of new capabilities with minimum interruption or standardized configurations for specific organization and echelon levels. The ability to have a small system facilitate intelligence gathering and transmitting that information in a covert manner in hostile situations has also been identified as a gap in the current way the RCCs conduct business. These gaps have been identified as critical elements to the success of any small C2 system that has to be utilized by first responders.

2.4 DETERMINING THE STAKEHOLDERS AND MISSIONS

As the principal organization responsible for the design and development of the RRK, the DJC2 JPO became the immediate stakeholder for the R2C2 team's integrated project. Mutual support by the R2C2 team and the DJC2 JPO ensured a constructive product for both parties. Continuous collaboration with members of the JPO provided guidance to portions of the study. This report and the analysis contained had been used to assist the SE efforts conducted by the DJC2 JPO for the RRK.

The research conducted by the R2C2 team spawned various interested parties throughout the NPS campus. Through collaborative efforts with these groups, the R2C2 project gained their support and interest. These groups included faculty and students involved in COASTS, TNT, and HFN. Input and assistance from the different groups provided valuable information to the technological aspect of the R2C2 study.

2.4.1 Regional Combatant Commanders (RCCs)

The ultimate stakeholders for the R2C2 are the users. In this case, the users for the R2C2 will be the RCCs. The RCCs were chosen as the users for the R2C2 because the system was a subset of the larger DJC2 system. The user's feedback session, held by the JPO identified four potential users of the R2C2: EUCOM, SOUTHCOM, PACOM, and CENTCOM. As the study progressed, Northern Command (NORTHCOM) and SOCOM were added to the list of stakeholders. Their addition was due to the lack of capabilities available for personnel responding to disaster relief situations such as

Hurricane Katrina. All their inputs to the requirements, scenarios, and forecasted use of the R2C2 were critical in determining the scope of the R2C2's capability.

2.4.2 Missions of the R2C2

Having various stakeholders proved to be slightly more difficult than predicted because each RCC had specific missions and tasks for their particular AOR. Standard military operations (i.e., war, NEO, and antiterrorism) did not vary between RCCs; however, research found that there were complexities and variances with the carrying out of region-specific missions that fell under their responsibility. More specifically, factors such as weather, terrain, operating environment, and geopolitical climate contributed to the inconsistency between RCCs. Designing a system that could meet all these missions proved to be beyond the scope of the study. Therefore, from the number of military operations supported by the RCCs, different missions were chosen for examination. These scenarios were picked for their relevance to the RCC's regions and their likeliness of occurrence. More on scenarios development is covered in the next section.

2.5 DETERMINING POTENTIAL SCENARIOS

The RCCs need to be prepared for numerous missions that require different levels of C2 support and span different geographical regions. These differing expectations or stresses on the role of the R2C2 must be studied in order to architect a system that best suits the requirements. The process of predicting and listing all the possible scenarios is beyond the scope of this study. Hence, rather than be prescriptive, we recommended the following two-pronged approach in our system engineering process:

- Devise a methodology to analyze how different scenarios will stress the R2C2.
- Apply this approach to the most probable scenarios that we have identified together with DJC2 JPO to test its relevancy.

2.5.1 The Methodology – Scenario Stress Matrix

We adopted a matrix comparison methodology in our analysis of the degree of stresses that different scenarios apply on the R2C2. A matrix template was formed with

rows and columns for comparison. The rows indicated the types of possible missions or scenarios that RCCs may encounter. The columns were various considerations that may incur stresses on the R2C2 when it needs to be deployed.

The types of possible missions should follow directly from the range of military operations that will be expected. The best guidance was the Doctrine for Joint Operations,[25] where this range was defined. This has been reproduced in Table 1 as a reference and the terms "War" and "MOOTW" are defined below.

	Military Operations	**General U.S. Goal**	**Examples**
War	War	Fight and Win	Large-scale Combat Operations: Attack/Defend/Blockades
Period of Tension "POT"	Military Operations Other Than War	Deter War and Resolve Conflict	Peace Enforcement/NEO/Strikes/Raids/Show of Force/Counterterrorism/Peacekeeping/Counterinsurgency
Peace		Promote Peace and Support U.S. Civil Authorities	Antiterrorism/Disaster Relief/ Peace-Building/Nation Assistance/Domestic Support/Counterdrug/NEO

Table 1: Range of Military Operations

War (Fight and Win). In such cases, the goal is to "win as quickly and with as few casualties as possible, achieving national objectives and concluding hostilities on terms favorable to the U.S. and its allies."[26] Deploying R2C2 in such scenarios would incur high risks and potential conflicts could be expected. Hence, the appropriate level of security protection must be allocated to ensure the safety and success of the deployment.

Military Operations Other Than War (MOOTW). MOOTW are an aspect of military operations that focus on "deterring war and promoting peace."[27] These can be subdivided into either the involvement or noninvolvement of the use or threat of force.

- **MOOTW involving the use or threat of force.** The general goals of U.S. military operations during such periods are to support national objectives, deter war, and return to a state of peace. Such operations involve a greater risk that U.S. forces could become involved in combat

[25] Chairman, Joint Chiefs of Staff, Joint Publication 3-0: Doctrine for Joint Operations, Chapter 1, "The Strategic Context," September 2001, p. I-2.

[26] Chairman, Joint Chiefs of Staff, Joint Publication 3-0: Doctrine for Joint Operations, Chapter 1, "The Strategic Context," September 2001, p. I-3.

[27] Ibid., p. I-3.

rather than operations conducted to promote peace. This **Period of Tension (POT)** is often sensitive, as great efforts are placed in deterring any probable transition into a war. Security requirement will also be high when deploying the R2C2 since hostile forces will be expected in the region. Examples of such operations include combating terrorism, enforcement of sanctions, enforcing exclusion zones to prevent civil unrest, and NEO.

- **MOOTW NOT Involving the use or threat of force.** These operations occur in **Peace** time and do not usually involve combat, but there is potential for them to escalate into armed conflicts. Hence, military forces deploying the R2C2 must always be prepared to protect themselves and respond to a changing situation. Such operations include HA/DR, counterdrug operations, pandemic control, evacuation of noncombatants, and peacekeeping. Such operations are often "Joint" in nature and most also involve multinational cooperation among different military forces and NGOs.

With these categories of military operations defined, the amount of stress on deploying the R2C2 for each operation was analyzed based on a series of stress points. For our context, the Mission, User, and In Situ stress points represent the three categories of concerns that would affect the design of our R2C2 system. Mission stress points refer to considerations that spin off from different mission requirements. User stress points are the expectations of stakeholders and In situ stress points are more geographically related and are concerned more with the in-theater challenges facing R2C2 deployment. A list of each stress point and corresponding considerations is provided in Table 2 for illustration.

No.	Considerations	Explanation	Grade[(1)/(2)/(3)]
Mission Stress Points			
1	Response Time	How much time is available to set up the R2C2?	Adequate (> 1 day)/ Urgent (< 1 day)/ Immediate (< 6 hrs)
2	Probability of Occurrence	What are the likelihood and frequency of this specific scenario occurring in the near future?	Low/Medium/High
3	Impact	What is the impact if such an R2C2 is not deployed to the scenario site?	Localize/Regional/ Widespread
4	Prior Intelligence/ Information	Is prior information about the area of operations critical in deploying the R2C2?	Not required/ Bonus/Necessary
User Stress Points			
5	User Expectation	How detailed are the Inputs, Process, and Output? How frequently are they transmitted?	Low/Moderate/High
6	Stakeholders	Who directly or indirectly need the information provided by the R2C2?	Intra-agency/ Inter-agency/Coalition
7	Complexity of Operation	Who will be involved in using the system for regular updates and what skill set do they need?	Small (2 px)/Medium (platoon)/Large (company and beyond)
8	Duration (stay + ops time)	How long will the R2C2 be deployed (including stay time and operations time)?	Short (< 1 week)/ Medium (< 1 month)/ Long (> 1 month)
In Situ Stress Points			
9	Environment	What is the environment (e.g., counter Information Assurance, troop safety, political sensitivity) surrounding the R2C2 deployment?	Peaceful/Tension/ Hostile
10	Infrastructure	What are the supporting elements (e.g., logistics, power supply, network maturity, communications availability) that will be available for usage?	Supported/ Supplementary/Poor
11	Trafficability	How convenient is it to deploy/extract the R2C2 to/from the designated spot/location?	Supported/ Supplementary/Poor
12	Special Requirements	Are there other special requirements to be met under this scenario? If so, how extensive are these additional efforts or resources?	None/Some/Lots of resources and efforts

Table 2: Scenario Stress Matrix Stress Points

Referring to Table 2, the grading provides a pseudo-quantitative measurement of the stress level of each scenario, with respect to each consideration in the stress points. The larger the number, the higher the stress level that a particular consideration places on the specific scenario. Referring to Appendix A, Scenario Stress Matrix, provides a useful and direct approach to compare the scenarios on the extent of each consideration affecting the R2C2 deployment. However, it must be cautioned that there is little meaning in summing all the figures for each scenario to an eventual figure, as each scenario is unique and placed different emphasis and weights for each consideration. To summarize, the Scenario Stress Matrix provides a qualitative appreciation between

scenarios and consideration (stress points) and the pseudo-quantitative measurement serves as a guide for comparison across scenarios for each consideration.

2.5.2 Applications to Probable Scenarios

The preceding discussions proposed three probable types of missions: War, POT, and Peace. These form the basis of choosing the most common scenarios to deploy the R2C2. To encompass the three areas, five missions were chosen to represent the flexibility of the R2C2. The geographic locations were arbitrarily picked to support the missions for educational purposes only.

For the "War" missions, a potential deployment to Iran has been selected. This is because Iran does pose a significant threat in the Middle East. From lessons learned in Operations Enduring Freedom and Iraqi Freedom, implementation of an R2C2 was studied to gage the potential uses in a similar environment. Conscious of the sensitivity in choosing Iran, the R2C2 team strictly considered the capabilities of an enhanced C2 system not the probable tactics of U.S. forces in an Iranian conflict.

For the "POT" missions, possible civil unrest in Ivory Coast and counterterrorism operations off the southern Philippines are appropriate scenarios that exemplify the potential security tensions that such missions stress on the R2C2. Aside from the "Peace" missions, these types of missions presented the next highest likelihood of operational use for the R2C2 system.

For the "Peace" missions, the R2C2 system supports disaster relief in Central America and pandemic control efforts in Singapore to emphasize the difficulties in remote C2, even in a peaceful environment. Lessons learned from Hurricane Katrina and the Boxing Day Tsunami provided insight into the complexities faced in aiding victims of natural disasters. Collaboration of information between civil, military, and outside agencies in a coordinated effort proved very difficult. Because of their probability of occurrence, the R2C2 team chose these two missions to further investigate the effectiveness of the R2C2.

2.6 MISSION SCENARIOS

The scenario stress matrix guided us to approach the problem of identifying the RCCs' scenarios systematically by comparing the scenarios individually with the potential stress points on the R2C2. Using this methodology, we have come up with five probable missions to be focused on: Pandemic, Disaster Relief, Counterterrorism, Civil Unrest, and Deployment.

2.6.1 Pandemic Scenario

Avian influenza (or "bird flu") is a contagious animal disease that infects birds and some mammals. Wild waterfowl, especially ducks, are a so-called natural reservoir of influenza viruses, including bird flu. The birds carry the virus without displaying any symptoms of the disease and can spread the virus over great distances, while remaining healthy themselves. The severe form of the disease, which is known as "highly pathogenic avian influenza," is extremely contagious and has been the source of numerous epidemics among domesticated birds.[28]

Although frequently deadly for poultry, past avian influenza viruses have rarely caused severe disease in humans. However, in 1997, a highly pathogenic strain of bird flu known as H5N1 jumped from birds to humans during an outbreak among poultry in Hong Kong. The 1997 event was notable for two reasons. First, molecular studies indicated that the genetic makeup of the human and avian viruses were virtually identical, indicating direct transmission from birds to humans. Second, the H5N1 virus caused severe illness with extreme mortality among humans: of the 18 persons known to be infected, 6 died. The outbreak ended after authorities slaughtered Hong Kong's entire stock of poultry.

Since the 1997 episode in Hong Kong, there have been several outbreaks of the H5N1 influenza around the world. In 2004 and 2005, the H5N1 virus spread among poultry populations in Southeast Asia and affected Vietnam, Japan, Korea, Thailand, Laos, Cambodia, Indonesia, China, and Malaysia. More recently, the virus has shown up in Russia, Kazakhstan, Turkey, and Romania.

---

[28] World Health Organization, Avian Influenza Report: Assessing the Pandemic Threat (Geneva: World Health Organization, January 2005).

The number of human cases of the H5N1 virus has also grown. Between January 2004 and August 2005, there were 112 human cases of H5N1 avian flu (in Vietnam, Thailand, Cambodia, and Indonesia) that resulted in 57 deaths. Nearly all of the human cases resulted from close contact with infected birds.[29] There is evidence, though, of at least one case of probable human-to-human transmission, and some experts suspect that a few other cases of human-to-human spread of the H5N1 virus have occurred.

Based on the experience of the Severe Acute Respiratory Syndrome (SARS) in 2003, a H5N1 flu pandemic is expected to spread widely across national borders very rapidly. The most immediate impact of a pandemic would be a surge in demand for medical services, and keeping track of where the disease is and where it was going would be difficult. As the pandemic progresses, international travel would dramatically decline, as people avoid avian flu "hotspots" and governments issued travel warnings. Business confidence would be dented and economic activity generally slows down, thereby affecting the world economy. As such, it is important that the U.S. work with its coalition partners in curbing the spread of the virus at the earliest possible opportunity.

For our scenario, last month several workers in a printing company in Singapore were diagnosed with the H5N1 virus. Investigations revealed that one of the workers had visited his family on a poultry farm the weekend before. The other workers were not known to have any direct contact with live birds or poultry. This could signal the first case of massive spread of the H5N1 virus variant that is capable of human-to-human transmission. Shortly thereafter, a lady fell ill at the Tan Tock Seng Hospital in Singapore and was diagnosed with the H5N1 virus. She made regular trips to regional countries for business and had just returned from a trip to Thailand. Similarly, she has had no known contact with live birds or poultry during her trips. As part of the national response plan, designated medical institutions in Singapore were put on alert[30] and a

---

[29] World Health Organization, Avian Influenza: Assessing the Pandemic Threat (Geneva: World Health Organization, January 2005).

[30] News@AsiaOne Report, 5 April 2005, "Singapore outlines flu pandemic preparedness plans; to hold emergency drill," http://hosted.ap.org/dynamic/stories/A/AS_MED_SINGAPORE_FLU_ PREPAREDNESS_ASOL- ?SITE=ASIAONE&SECTION=SOUTHEAST&TEMPLATE= DEFAULT&CTIME=2006-04-05-02-02-35.

Contact Tracing Center was set up to monitor the development of the spread of the virus and to commence contact tracing, starting with the lady business traveler and establishing all the persons she came in contact with for the past week.

2.6.1.1 Mission

PACOM decided to deploy an R2C2 crew to Singapore to provide an accurate situational awareness picture on the spread of the H5N1 virus across Southeast Asia. If required, this R2C2 crew could be later augmented to form a Regional Coordination Center. Accurate monitoring of the situation is crucial in formulating an appropriate response plan and deploying mobile medical facilities where necessary.[31]

The mission is to make use of all available information resources in order to compile an accurate situation awareness picture on the extent of the spread of the H5N1 virus in Southeast Asia. Identifying and establishing contact with the various sources is critical in gaining the most accurate information for the RCC. Figure 4 depicts the CONOPS for the Pandemic scenario. Local communications, depicted by blue dashed lines, are made with the R2C2 scouts, as well as the police, fire, and medical departments of Singapore. Red dashed lines illustrate long haul communications with PACOM, medical facilities supporting operations from the U.S., and an en route Expeditionary Strike Group (ESG). An orange line represents the communications with NGOs, such as the Red Cross and WHO, which may possibly communicate locally or remotely.

[31] "A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues," 8 December 2005, http://www.cbo.gov/ftpdocs/69xx/doc6946/12-08-BirdFlu.pdf. Last accessed in February 2006.

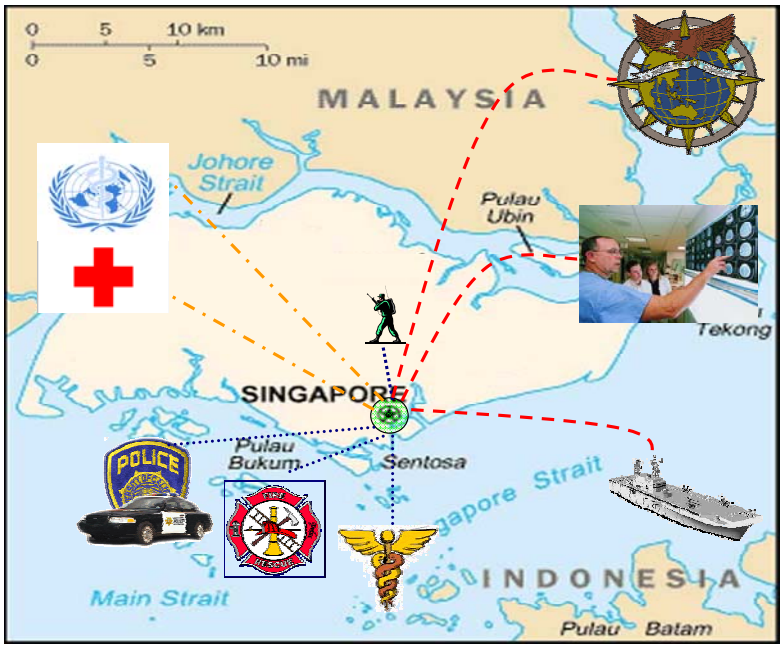


Figure 4: Pandemic Concept of Operations

From Hawaii, the R2C2 crew is to deploy to Commander Logistics Western Pacific (COMLOGWESTPAC) in Singapore. Once at COMLOGWESTPAC, the R2C2 crew will be supported with the necessary materials and facilities to conduct continuous operations. A Civil-Military Operating Center (CMOC) will be established on base as a central hub for information gathering and distribution. Access to the CMOC will be granted to civil authorities and NGOs on a need to know basis to regulate security and information trafficking.

Upon establishing reachback capability, certain R2C2 scouts will be deployed to the major hospitals in Singapore. From the hospitals, all data from reported H5N1 cases will be collected minus personal patient information. This data shall include statistical information such as, but not limited to, the number of avian flu cases, rate of infections diagnosed, and death rate. Also, virus imagery that is available is collected for transmission back to the U.S. for examination and DB building. The majority of the data collected by the scouts is passable through voice situational reports (SITREPs) to the R2C2. Imagery or bulk data information will be physically brought back to the CMOC for transmission via long haul connection.

The remaining scouts will establish contact with agricultural officials to gather data. Their responsibility will be to collect information on the poultry industry.

Reported poultry deaths and the regions of occurrence will be the primary information these scouts are gathering. Their information will be passed through voice SITREPs as well. To mitigate the chance of infection, the scouts are not authorized to visit any poultry farms. Data collection will be limited to information reported to the agricultural offices.

At the CMOC, the R2C2 operators will conduct collaborative efforts with local and NGO representatives. The R2C2 will provide Internet access for the NGOs to collaborate with their parent organizations. An increase in information sharing and coordinated efforts is the objective by providing this capability. Bulk data and imagery collected by the scouts will be passed by the R2C2 from the CMOC to PACOM, ESG, and the U.S. medical facilities. Coordination with the ESG and the R2C2 will be done in order to provide any medical support needed as identified in the information gathered by the scouts.

2.6.1.2 Complexities

The small geographic region of Singapore promotes pockets of densely populated areas. In heavily populated sections, the spread of the H5N1 virus has a higher probability of transmission. Investigating a communicable virus across the region increases the risk of acquiring the virus for the R2C2 crew. The utmost levels of precaution must be taken by the R2C2 crew and the various organizations they will be working with. In addition, once their mission is complete, the crew members of the R2C2 must be quarantined as a preventative measure.

Depending on how the RCC decides to augment the R2C2 crew, typical crew members will have little to no medical experience. Quick, informative training on H5N1 and safety measures will need to be done for the crew members prior to deploying. If the R2C2 crew is not augmented with medical personnel, support from local medical agencies will be critical. Working through patient confidentiality clauses in order to gain access to data is an issue that needs to be further investigated. Support from stateside medical facilities will be important to help guide the crew in their information collection.

2.6.1.3 Assumptions

The first assumption made for the Pandemic scenario is that the R2C2 crew will be properly trained prior to deploying to Singapore. If deployed without an augmented medical team, the R2C2 team will be collecting data with minimal medical backgrounds. Ancillary to the training, the crew will be adequately outfitted with the proper safety equipment and protective gear for dealing with the avian flu virus. A full-blown outbreak has not yet occurred; however, for crew safety, all risk factors must be mitigated.

That notification of deployment to the other in-theater agencies of Southeast Asian countries will be undertaken by PACOM is a second assumption. The onset of a pandemic involves the probability of spreading to other countries. In the region of Southeast Asia where Singapore is located, the relative closeness of her bordering nations is a concern for virus containment. PACOM shall undertake the diplomatic responsibilities of coordinating with bordering nations and their health organizations.

The third assumption made was that Singapore has no objection to the presence of additional U.S. forces in country in the joint combat against the pandemic outbreak. Working together with the Singaporean government and military in a joint effort makes for an easier situational evaluation. The U.S. and Singapore have maintained a healthy relationship diplomatically and militarily over the years. The U.S. presence to support the people of Singapore would only strengthen the existing bond between the two nations. The small footprint of military personnel also adds to the acceptance of the R2C2 crew.

It is also assumed that COMLOGWESTPAC is self-sufficient in terms of infrastructure support such as power, network connectivity, and physical protection. Having the dedicated power supply, shelter, and infrastructure to operate within the CMOC improves the operational capability of the R2C2 system. Also, the support of COMLOGWESTPAC to provide services enables the CMOC's existence. The purpose of the CMOC is to promote the collaborative and distributive efforts of multiple organizations outside of the military. Providing this capability will show the Singaporean Government and other nations of Southeast Asia the level of commitment of the U.S. Government in the region.

2.6.2 Disaster Relief Scenario

El Salvador sits on an active fault line that produces an average of two earthquakes a year registering over magnitude five.[32] In the next 20 years, there is a 50% (±30%) probability that San Salvador, El Salvador will have an earthquake of the magnitude 7.75 ± 0.3.[33] The red circles shown in Figure 5 depict earthquakes registering over magnitude five near San Salvador and along the coast since 1980. Though earthquakes are frequent, those that measure above magnitude six cause immediate devastation to the country's infrastructure and significant loss of life. The last major earthquakes in January and February 2001, measuring 7.6 and 6.6 Mw, killed 1,259 people and destroyed 149,563 homes.[34]

Figure 5: Earthquake Epicenters Around El Salvador Since 1980[35]

---

[32] U.S. Geological Survey, http://earthquake.usgs.gov/regional/world/central_america/density.php. Last accessed in March 2006.

[33] Randall A. White, "Seismic History of the Middle America Subduction Zone Along El Salvador, Guatemala, and Chiapas, Mexico: 1526-2000," Manuscript accepted 16 June 2003, http://www.gsajournals.org/gsaonline. Last accessed in March 2006.

[34] Red Cross Red Crescent Operations Update, http://www.ifrc.org/cgi/pdf_appeals.pl?01/020118.pdf. Last accessed in March 2006.

[35] Google Earth, Copyright 2006, Europa Technologies, Image Copyright 2006 Terrametrics. Last accessed on 5 April 2006.

This earthquake scenario is similar to the 2004 Boxing Day Tsunami that brought about a new sense of awareness regarding disaster relief. It was massive in scale and required relief operations that could match it in terms of size, complexity, and response. Although this experience has set new benchmarks for international cooperation, the need to have better coordination and information sharing and to operate in the field in a sustainable manner cannot be overemphasized.

International organizations and the U.S. are obliged to provide and offer humanitarian assistance and disaster relief to states in need. The desired outcome of the provided aid includes restoring social stability in the affected state. Even more so than social instability, political instability in disaster regions may spill over to neighboring nations. The greater the disaster, the greater the chance of political instability arising. Again, by providing aid to a state in need, IOs and the U.S. can speed the return to normalcy and help avert any potential economic downturn.

The approach to disaster relief can be categorized by three critical states: Disaster Strike, In-Theater Assistance, and Normalcy, going through two transition phases of Deployment and Reconstruction, with the eventual effect of capability build up. The event that triggers the entire relief effort is when disaster strikes, following which, relief efforts will be provided through the deployment of teams to render assistance at the relief sites (In-Theater Assistance). The objective is, of course, to bring the disaster-hit regions back to normalcy as soon as possible.

The core processes involved in this Deployment phase are impact analysis, scoping of relief efforts, and capabilities preparations specifically for resources and logistics. Impact analysis focuses on assessing the extent of damages from the unforeseen disaster, with reference to environmental factors, and also through constant feedback from the progress at the disaster sites. With the analytical results, the range and depth of relief support will be determined. A comprehensive plan is useless without the appropriate implementation. Hence, it is very important to step up relief preparations to ensure the availability, dependability, and capabilities of the resources provided. Finally, timely logistics support and transport of the necessary resources to the disaster sites are also critical to the relief efforts. Through in-situ insertion of an R2C2 crew to monitor the environment, we will be able to attain the level of time critical awareness.

It is important to appreciate that social and economic reconstructions are the focus in this Reconstruction phase. Economic reconstructions will focus on the "hardware" aspects, concentrating on building infrastructures that support basic needs. Social reconstructions tackle the "heartware" of the victims by providing them with moral support and counseling through this difficult and sensitive period. If there is no established communication system being setup, the R2C2 will continue to be the source of information gathering to aid decision makers in the journey to normalcy.

2.6.2.1 Mission

A U.S. military Forward Operating Base (FOB) is located at the El Salvador International Airport, located approximately 25 miles southeast from densely populated San Salvador. The FOB supports a small detachment of counterdrug air assets and supporting staff. In our scenario, a magnitude 8 earthquake strikes between San Salvador and the FOB, devastating the region and triggering massive landslides. Power and local communications are disrupted and major roads are impassable. SOUTHCOM has lost communications with the FOB and the U.S. Embassy and has ordered an R2C2 crew to deploy to the region to determine the status of the FOB personnel and provide disaster relief assistance.

Figure 6 depicts the CONOPS for this scenario. The blue lines represent local communications between the scouts and the R2C2 and the red lines represent long haul communications back to the RCC or the ESG. Unable to contact the FOB or the Embassy, SOUTHCOM alerts an R2C2 crew, consisting of intelligence personnel, communication technicians, and scouts, to prepare for operations in El Salvador. After circling and taking pictures of the El Salvador International Airport, the military helicopter determines a suitable landing site and drops off the R2C2 crew. The R2C2 crew locates the FOB personnel near airport structures and begins setting up the R2C2 system.

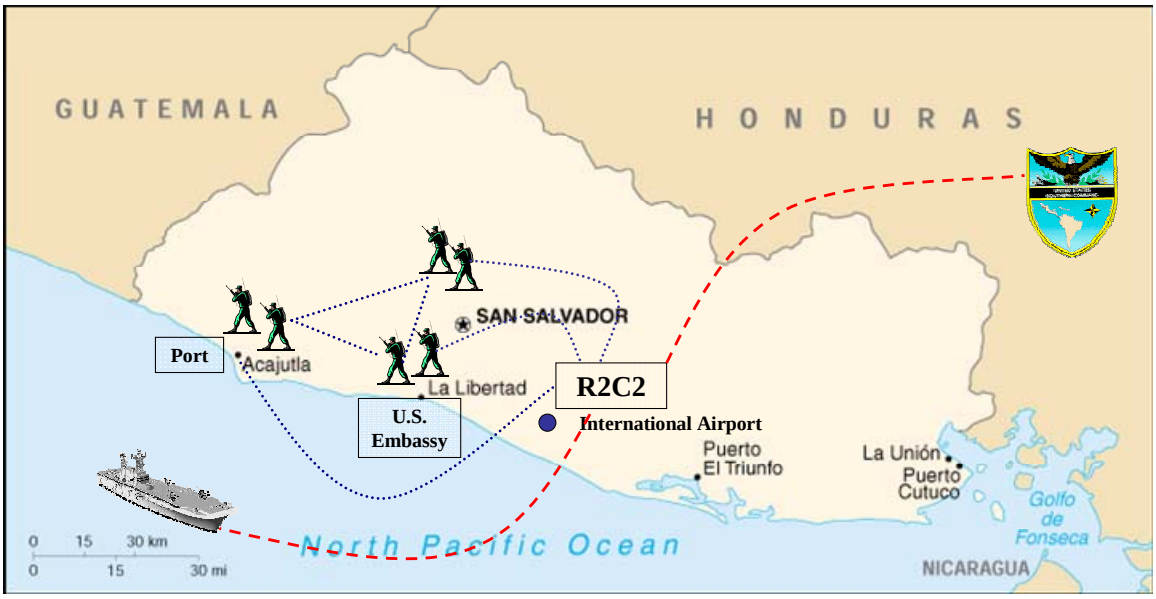


Figure 6: Disaster Relief CONOPS

Initially, no power is available at the airport, so organic power sources transported by the R2C2 crew are used. Voice and data communication checks are established with the R2C2 and SOUTHCOM and the R2C2 and the scouts. The initial situation report (SITREP) to SOUTHCOM includes the status of the FOB personnel, video clips or pictures of the coastline and the airport, and immediate first aid requests.

The R2C2 crew starts relocating the scouts to the San Salvador fairgrounds, the Embassy in La Libertad, and the Port of Acajutla located approximately 20, 25, and 35 miles away, respectively, from the airport. After the 2001 earthquakes, local agencies, International Organizations, and NGOs assembled at the fairgrounds to organize the relief effort. The scouts assigned to the fairgrounds will help establish a CMOC and report on search and rescue requirements, medical needs, local population morale, and physical security updates. As critical pictures of the devastated region become available from the RCC, scouts will provide these images to the CMOC. The scouts assigned to the Embassy will report on the status of Embassy personnel and equipment, work to restore Embassy communications, and help the Embassy execute the natural disaster plan. The last scout team will travel to the Port of Acajutla to determine port damage and security for the ESG. The ESG is en route, carrying relief supplies, and is expected to arrive in five days. The ESG has many air assets to provide the much needed logistic support to deliver supplies and transport evacuees.

During the first 24 hours of the operation, the scouts are reporting hourly to the R2C2 and the R2C2 is reporting bi-hourly to the RCC. At the beginning of the second day, the FOB personnel are able to provide mobile generators used by the aircraft and support equipment to power the R2C2. Throughout the remainder of the operation, SITREPS continue bi-hourly from the scouts to the R2C2 and reports to the RCC and ESG are sent three times a day.

2.6.2.2 Complexities

This is a time critical surge operation that requires sudden and massive support. As a result of the sudden congregation of large amounts of resources (manpower and materials) in a haphazard manner, the relief operations are constantly subjected to uncertainties from the unfolding situation. During the Tsunami relief operation, over 40 countries and 700 NGOs contributed in various ways such as providing manpower, supplies, and pledges of funds for the relief and reconstruction work. Coordination among the various parties was a major challenge during the Tsunami and will be a challenge in our scenario. Potential tension may arise between civilian and military organizations due to different requirements, expectations, and operating norms. The U.S. military must patiently work with the civilian organization leading the disaster relief to ensure effective and efficient use of military resources.

Physical security currently poses a challenge to the U.S. military, visitors, and locals in El Salvador. The U.S. Embassy considers El Salvador a critical crime-threat country. Armed assaults, carjackings, and kidnappings, as well as petty crimes, are prevalent throughout El Salvador.[36] There is potential for civil break down after a natural disaster and criminals might hijack the relief supplies or harm relief personnel.

The operating environment will be difficult because the infrastructure (e.g., communications, water, sanitation, and power supplies will likely be devastated. It will be difficult to determine the best logistic routes due to road destruction and potential physical threats from looters. Power grids will be damaged and gas needed for generators will be difficult to find.

---

[36] United States Department of State, http://travel.state.gov/travel/cis_pa_tw/cis/cis_1109.html. Last accessed in March 2006.

2.6.2.3 Assumptions

Three assumptions have been made for this scenario: 1) The El Salvadoran military will provide transportation for the scouts; 2) Generator power is available after the first day of operations; and 3) The ESG is en route and expected to arrive in five days. Since the El Salvadoran military has a base at the International Airport, it is assumed that they would be able and willing to provide transportation to the scouts and provide local protection as required. Since the FOB utilizes gas-powered generators to power aircraft on the deck and support equipment, the second assumption—that the R2C2 can utilize this power source after the first day of R2C2 operations—was determined. Though gas will be scarce, there will likely be enough gas at the airport to power the generators. The final assumption is based on the Navy's quick reaction in deploying USS LINCOLN to Southeast Asia to provide disaster relief after the Tsunami. For this scenario, an ESG based in San Diego quickly stocks disaster relief equipment and supplies and transits down to El Salvador in five days.

2.6.3 Counterterrorism Scenario

The most southern province of Basilan in the Philippine Islands (Figure 7) has been devastated by terrorism for many years. A significant reason behind the terrorism against the government is due to inequality toward the Muslim community. Muslims comprise 71% of the population in the southern provinces; however, the Christian population owns over 75% of the land and the Chinese control 75% of the businesses. This region is surrounded by oceans, rich land, and untouched forest, yet over 75% of the food consumed is imported from neighboring provinces. Although food is grown in the region, it is largely cultivated for export.

The Comprehensive Agrarian Reform Law of 1988 was passed to distribute the land in the region; however, the Muslim population was again over looked, resulting in family feuds and clan conflicts.[37] The inequality toward the Muslim population and the influx of Christians from the north, forcing the Muslims to be a minority in their own land, resulted in the formation of the Moro National Liberation Front (MNLF), whose

[37] Jose Toresse, Jr., "Basilan: Abu Sayyaf's Birthplace," ABS-CBN News Report, http://www.abs-cbnnews.com/images/news/microsites/abusayyaf/basilan.htm. Last accessed in February 2006.

purpose was to develop an independent Muslim nation. The MNLF eventually negotiated a peace settlement with the Philippine Government; however, one group did not agree with the conditions of the settlement and separated from the MNLF, forming its own organization, which became the Abu Sayyaf Group (ASG). The initial goal of the ASG was to separate from the Christian majority, but when the ASG demanded separation and was ignored, terrorism began around the country with the goal of promoting an independent Islamic state in western Mindanao and the Sulu Archipelago.[38]

The U.S. State Department formally designated Abu Sayyaf a terrorist organization in 1997, which enabled the U.S. Government to freeze any assets the group had in the United States.[39] Aburajak Janjalani was leading the terrorist factions, but after his death in 1998, his brother Khadafi Janjalani became the group's leader. The ASG has been funded by kidnapping ransoms and extortion; one such incident being the "April 2000 kidnapping of Western tourists and a resort employee in Malaysia. . . [which] ended in a multimillion-dollar ransom payment negotiated by Libya and reportedly paid by European governments."[40]

After the attack on the World Trade Center on September 11, 2001, the United States became very involved in the fight against terrorism. The United States ordered SOCOM to send troops to the Philippines to assist in the training of their military forces. U.S. special operations forces (SOF) have been in the Philippines conducting exercises on Basilan Island with the Philippine military and constantly training and preparing them for combat in the fight against terrorism.

While conducting exercises in the Philippines, U.S. SOF received intelligence of increased Abu Sayyaf activity, indicating that the group may be planning a terrorist attack in Manila and that a high ranking terrorist leader is possibly in the region (in a camp near Buriasan; see Figure 7). The Philippine Government was made aware of the intelligence report and requested U.S. support to survey and possibly eliminate the terrorist leader.

---

[38] Jose Toresse, Jr., "Basilan: Abu Sayyaf's Birthplace," ABS-CBN News Report, http://www.abs-cbnnews.com/images/news/microsites/abusayyaf/basilan.htm. Last accessed in February 2006.

[39] C.S. Kuppuswamy, "Abu Sayyaf: The Cause for the Return of U.S. Troops to Philippines," South Asia Analysis Group Paper, No. 417, 28 February 2002.

[40] Council on Foreign Relations, Terrorism: Question and Answer, Abu Sayyaf Group: Philippine Islamist Separatists, http://cfrterrorism.org/groups/abusayyaf2.html. Last accessed in February 2006.

Figure 7: Philippine Islands

2.6.3.1 Mission

In the continuing fight against terrorism, the United States and the Philippine Government agreed to tackle terrorism in the Philippines head on. A team of U.S. and the Republic of the Philippines (RP) SOF left the Balikatan exercises being conducted on Basilan Island and were assigned this coalition mission. The SOF team, deploying with the C2 capabilities of the R2C2, will covertly move from Basilan Island to Mindanao Island (the location of the terrorist camp) by small boat. SOF team members will conduct surveillance in and around Buriasan and pass situation awareness data to the R2C2 operators. From the operators, the collected data will be transmitted back to SOCOM. Due to the high level of secrecy involved in this mission, the SOF will inconspicuously collect and transmit Human Intelligence found in Buriasan to SOCOM. Utilizing their Filipino counterparts as translators, the U.S. SOF team is able to gather the necessary intelligence from the local population of Buriasan.

After the Abu Sayyaf training camp is located near Buriasan, the coalition SOF team will conduct surveillance. Scout members of the team will deploy and

surround the camp to gain the most information possible. Radio transmissions will be made between the scouts and the R2C2 to provide intelligence. Digital imagery will be taken by the scouts of the camp whenever possible. Identifying the High Value Target (HVT) is their primary mission. Subsequent to that, intelligence on camp size, training tactics, and personnel size is gathered. Live video, which positively IDs the HVT in the camp, will be transmitted back to SOCOM when available, and then the team will await confirmation and follow-on orders. Figure 8 represents the CONOPS for this mission. The blue lines indicate the local communication between the scouts and the R2C2. The red line from the R2C2 represents the long haul communication between the R2C2 and the RCC.

Figure 8: Counterterrorism Concept of Operations[41]

2.6.3.2 Complexities

In order to carry out its missions, the U.S.-RP team will have to covertly move from Basilan to Buriasan without alarming the High Value Target (HVT) in the country. The short timeline the team has to complete the mission forces them to move

[41] Google Earth, Copyright 2006 Europa Technologies, Image Copyright 2006 Terrametrics. Last accessed on 25 May 2006.

quickly, which may increase the chance of mistakes. The actual location of the terrorist camp is not known at the start of the operation. Gaining that information from the citizens of Buriasan without someone notifying local terrorists adds difficulty to the mission. This mission is designed to be carried out during nighttime, which places an added strain on the system with regard to power, as it cannot use a generator; the operation's length is considerable; and the team can only carry so many batteries with them. The R2C2 system will have to be supplied with organic power that is deployed with the system, where it can be plugged into an inorganic power supply. The U.S.-RP team would have to covertly locate and monitor the activities of the terrorist camp, and afterwards be able to transmit that information to SOCOM within the allotted power and bandwidth requirements.

Mobility of the team will be an issue. Since the location of the camp is unknown, the U.S.-RP team may have to solicit transportation from locals in order to arrive at the objective in a timely manner before the HVT leaves the area. Failure to locate the HVT before he leaves the area will result in mission failure, even though the team may still be able to foil the plans of the terrorists. The covert movement of scouts to and from the R2C2 takes time, and the more they have to move to pass data, the greater the risk of alerting the terrorist camp to their presence.

2.6.3.3 Assumptions

The first assumption is that the intelligence received by the U.S. Government is credible and accurate, giving the U.S.-RP credible information from which to operate. Secondly, it is assumed that the Philippine Government supports the coalition team and their efforts. Thirdly, it is assumed that the Buriasan locals are cooperative with U.S.-Filipino forces. Our fourth assumption is that the Buriasan locals are also aware of terrorist activities and know where the terrorist training camp is located and they can confirm the arrival of a potential HVT in the region. The final assumption is that the U.S.-Filipino forces have been conducting exercises utilizing the capability of the R2C2 in the Balikatan exercise; therefore they are well versed in its capabilities and how to operate it.

2.6.4 Civil Unrest Scenario

For over three decades, after its independence from France in 1960, Côte D'Ivoire (Ivory Coast) was a model of political stability and economic prosperity under its then President, Felix Houphouet-Boigny. It avoided many of the pitfalls that plagued other African nations that experienced the difficulties of sovereignty.

Ivory Coast (Figure 9) is separated by religious principles with a predominantly Muslim north and a predominantly Christian South. Houphouet-Boigny, with his strong leadership abilities, managed to unite the country under a single government. During his tenure, he forged close political ties with the West (United States), which sheltered Ivory Coast from the crises associated with assorted military uprisings and Marxist experimentations that characterized other countries in the region. Houphouet-Boigny's leadership made it possible for the Ivory Coast to focus on stabilizing its economy, thereby attracting investors from foreign countries and making it the largest producer of cocoa not only in the region, but in the world.

Figure 9: Ivory Coast on the Continent of Africa

After the death of Houphouet-Boigny in 1993, Henri Konan Bedie became his successor. He faced an array of problems "including economic pressure from falling world market prices for cocoa and coffee, internal corruption that steeply reduced foreign

aid and a mounting political opposition."[42] During his tenure, Mr. Bedie implemented laws that prevented his then rival, Allassan Ouattare, from running in the presidential elections. In addition, he also instituted a policy that prevented anyone of foreign parentage, (i.e., both parents not of Ivorian descent, and who have never held nationality of another country) from running in presidential elections.

> . . . [the] Supreme Court disqualified all of the candidates from the two major parties by establishing the criteria that all candidates must have two Ivorian parents and never held a nationality of another country. This barred Ouattara and his Rally of Republicans party, or Rassemblement des Republicaines (RDR), from running after courts declared that his mother was from Burkina Faso.[43]

In 1999, a coup led by Army General Robert Guei overthrew the Bedie government. General Guei then formed his own government, promising to hold open elections in 2000; he also self-appointed his own Supreme Court. The court, selected by General Guei, upheld Mr. Bedie's policy regarding participation in the country's presidential elections.

Peace negotiations got underway in the beginning of April 2005, but October 2005 brought about additional frustrations for the rebels in the north when President Gbagbo cancelled the elections and invoked a law which he said allowed him to remain in office. The African Union recommended that Mr. Gbagbo stay in office an additional 12 months, and urged him to appoint a prime minister—acceptable to all parties to reduce tensions—with executive powers.[44]

For the R2C2 scenario, the failed peace negotiations between the rebels and the government led to presidential elections being canceled for the second consecutive year, and President Gbagbo's term being extended another 12 months. This decision further enraged the rebels who decided to take matters into their own hands. They launched an attack against the Gbagbo government with the intent of overthrowing it. As the fighting intensified, the rebels overwhelmed the UN/French peacekeeping forces patrolling the zone of confidence that separates the northern rebels from the southern government

---

[42] Global Security.org, Ivory Coast Conflict, http://www.globalsecurity.org/military/world/war/ivory-coast.htm. Last accessed in February 2006.

[43] Global Security.org, Ivory Coast Conflict, http://www.globalsecurity.org/military/world/war/ivory-coast.htm.

[44] BBC News, "Country Profile: Ivory Coast," http://news.bbc.co.uk/1/hi/world/africa/country_profiles/1043014.stm. Last accessed in February 2006.

controlled regions, forcing them to retreat. The rebel forces began a surge to the south toward the capital city of Yamoussoukro. As the rebels closed in on Yamoussoukro, the UN/French forces continued to fall back to the south. To help combat the rebel forces, the UN and Ivory Coast Government reached out to the U.S. for military assistance.

2.6.4.1 Mission

The growing tensions in Ivory Coast forced the French/UN forces to reach out to the United States to assist in the peacekeeping mission. The United States agreed to assist in the Civil Unrest operation, while conducting a NEO of the U.S. Embassy. U.S. military forces, with the C2 capability of an R2C2, will deploy two R2C2 crews: one in Yamoussoukro and the other in Abidjan in order to conduct surveillance in the rebel-held north (Yamoussoukro) and execute a NEO at the U.S. Embassy in the government-controlled southern region (Abidjan) of the country. The collected information will be transmitted via the R2C2 system, along with Situation Assessment data, to the RCC, depicted by the red line in Figure 10. The crews will simultaneously determine the political and social climate. These R2C2 crews must establish communications with the UN headquarters, the French, the other R2C2 crew and scouts in their region, as seen by the blue lines in Figure 10. Video imagery must be transmitted to the RCC that gives positive identification of rebel forces' headquarters and any top rebel force leaders. Digital imagery that identifies evacuation routes in Abidjan for NEO operations must be transmitted to the Expeditionary Strike Group (ESG) conducting the NEO. SITREPs will be transmitted on an hourly basis back to the RCC.

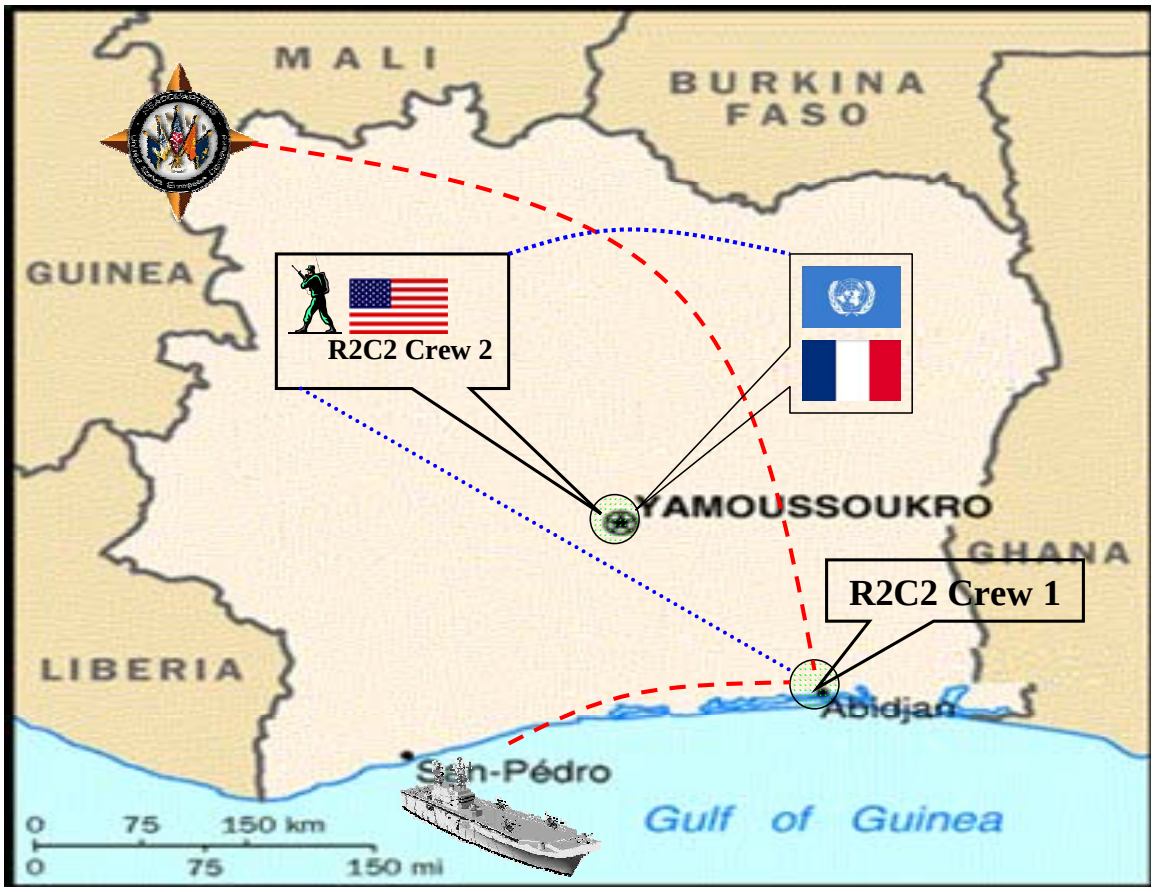


Figure 10: Civil Unrest CONOPS

2.6.4.2 Complexities

In order to carry out this mission successfully, the northern R2C2 crew will have to covertly move to Yamoussoukro and set up the system. Protecting the R2C2 system and personnel from the rebels will require additional personnel and protective equipment (i.e., dedicated force protection personnel and weapons for the system's operators). Placing the system in Yamoussoukro, where the UN/French troops are expected to see the most rebel activity, adds a calculated risk to the mission of the R2C2 crew in the north. The actual location of the rebel leaders is not known and gaining that information from the local population without someone notifying the rebel factions adds difficulty to the mission. The expected availability of power at the U.S. Embassy, adds more complexity to the operation. The R2C2 system will have to be deployed with organic power, be it batteries or other power sources, as reliable power may not available at the Embassy or in Yamoussoukro.

Mobility of the team will be an issue. Since the optimum location is unknown, the northern R2C2 crew may have to solicit transportation from locals, the UN, or French troops in order to arrive in Yamoussoukro and set up in a short amount of time.

2.6.4.3 Assumptions

The first assumption is that an ESG is en route to the region to provide a Marine Expeditionary Unit (MEU) for the NEO. Second, the Abidjan R2C2 crew will be able to communicate with the en route ESG. Third, the ESG will be prepared to provide information to support the R2C2 crews. Fourth, adequate to limited infrastructure is available for R2C2 operations in the city of Yamoussoukro.

2.6.5 Deployment Scenario

The Middle East is largely populated with an Islamic majority; however, Israel is one nation in the region with a large Christian population, and it has the backing and support of the United States. Along with supporting Israel, the United States has made significant efforts to promote democracy throughout the Middle East. Certain countries in the region have shown their disapproval of U.S. involvement there and its assistance to Israel.

The U.S.-lead War on Terrorism has sparked more hatred and rage among the Islamic community in the Middle East and around the world against the United States. After Operation Enduring Freedom and Operation Iraqi Freedom, some of the countries in the Middle East vowed to rid the region of American influence. Iran, with its highly sophisticated weaponry, is promoting anti-U.S. sentiments among other Islamic nations. Iran has publicly criticized the United States for their continued military presence in the region and vowed to eliminate the U.S. presence in the region by any means necessary.

For over two decades, in search of nuclear weapons, Iran has secretly conducted a uranium enrichment program in direct violation of International Atomic Energy Agency (IAEA) safeguards.[45] Iran does posses the largest inventory of ballistic missiles in the

[45] John D. Negroponte, Director of National Intelligence, "Threats, Challenges, and Opportunities for the U.S.," Annual Threat Assessment to the Senate Select Committee on Intelligence, 2 February 2006.

Middle East[46] and is known for its use of ballistic missiles as an integral part of strategic deterrence and, if necessary, retaliation. Within its inventory, Iran already has the capability of deploying a nuclear weapon by the missiles shown in Table 3. The danger of combining a nuclear weapon with its ballistic missiles creates a serious threat to the United States and to the nations bordering Iran.

Name	Range	Payload	Fuel	Source	Circle Error Probable (CEP)	Status
Scud B (Shahab 1)	Up to 300 km	770-860 kg	Liquid	Libya; North Korea	Approximately 1 km	Deployed
Scud C (Shahab 2)	Approximately 500 km	Approximately 700 kg	Liquid	North Korea	N/A	Deployed
Shahab 3	1,300 km	Approximately 750 kg	Liquid	Russia; North Korea	Approximately 3 km	Tested; a limited number may be deployed
Shahab 4	Between 1,800 and 2,000 km	Approximately 1,000 kg	Liquid	Based on Russia SS-4 "Sandal"	N/A	Uncertain
N/A – Not Available						

Table 3: Iran's Nuclear-Capable Ballistic Missiles

Intelligence has revealed that Iran also has ties with terrorist groups. Because of this they have been sanctioned as a State Sponsor of Terrorism by the United States. In their efforts to disrupt peace between Israel and Palestine, Iran has been a long time supporter of Hezbollah in Lebanon, a group which is responsible for more American deaths than any other terrorist organization apart from al-Qaeda.[47] During the development of a democratic state in Iraq, Iran has played a problematic role in supporting extremist groups and sectarian militias. Anticoalition efforts have been carried out by these groups and militias through the supplying of funds, weapons, training, and explosives from Iran. Iran is also responsible for at least some of the increasing lethality of anticoalition attacks in 2005, by providing Shia militants with the capability to build improvised explosive devices (IEDs) with explosively formed projectiles similar to those developed by Iran and the Lebanese Hezbollah.[48]

---

[46] John D. Negroponte, Director of National Intelligence, "Threats, Challenges, and Opportunities for the U.S.," Annual Threat Assessment to the Senate Select Committee on Intelligence, 2 February 2006.

[47] R. Nicholas Burns, Under Secretary of State for Political Affairs, "United States Policy Toward Iran," Opening statement before the House International Relations Committee, 8 March 2006.

[48] Ibid.

2.6.5.1 Mission

In the continuing fight against terrorism and the increase in tensions caused by Iran in the region, preparations have been made to conduct operations inside of Iran's borders by U.S. and coalition forces. No longer tolerant of the U.S. presence in the area, Iran has publicly threatened the U.S., focusing on harming American interests in the region. Knowing Iran's threat is valid, the United States initiates operations within the country. Swiftly and overwhelmingly, U.S. and coalition troops are able to secure the coastal city of Būshehr as well as Shirāz, approximately 100 miles to the northeast, within five days. These two cities ensure a safe logistics line to and from the Persian Gulf. With the two cities secure, CENTCOM deploys a single R2C2 crew into the operational area (OPAREA).

For the wartime deployment scenario, the R2C2 system will take on two missions. The primary mission of the R2C2 crew will be to determine a staging area for the RCC to set up its DJC2 core. Their secondary mission is to aid the local command element of the ground forces by enhancing the commander's C2 function, creating a more robust capability. In order to accomplish these missions, scouts will be deployed as part of the team to augment the R2C2 operators. Figure 11 depicts the CONOPS for the R2C2 crew during their missions. As seen, the red line depicts the reachback link to the RCC. The blue lines in the CONOPS represent the local communication provided by the Local Suite between the scouts, R2C2, and ground forces. Together, these missions stress the R2C2 system's ability to gather situational assessment, process gathered information, and provide long haul and local communications in an extremely austere environment.

Figure 11: Deployment CONOPS in Iran

Once local communications have been established between the R2C2 and the scouts, the scouts individually deploy with squad-sized infantry units to various locations throughout the city and its surrounding areas. Through voice communications, scouts will report back the position of any potential staging areas for a DJC2. Digital imagery of the possible locations will be taken by the scouts. All imagery taken by the scouts will be physically uploaded back at the R2C2. Transmission of various factors such as imagery, infrastructure, accessibility, protection, and habitability of different locations will be sent to the RCC for their approval via hourly SITREPs. A second message with only information pertaining to DJC2 sites will be sent to a construction battalion in the OPAREA who is responsible for the DJC2 staging area. This process will continue until a suitable site has been selected by the RCC, at which time the scouts will then be directed to secure that location.

Concurrently, as the scouts try to find an area for the DJC2 to operate in, they will report SITREPs to the R2C2 to build situational assessment. BDA will be done on the ground by the scouts through their digital imagery ability. The steady flow of information from the scouts raises the level of awareness in the AO. The information being reported back to the R2C2 is then shared with the ground element's commander and reported to the RCC. The software tools available on the R2C2 provide the RCC and the ground commander with a Common Operational Picture (COP) to aid in their tactical decision process.

2.6.5.2 Complexities

In order to carry out its missions, the R2C2 crew will first have to integrate with the ground forces already in Shirāz. Dedicated ground transportation from the coastline to the city of Shirāz will be necessary. Transportation is not an organic asset of the R2C2 system and will need to be provided by another source. Seamless integration will allow for a better COP for the ground commander, protection for the R2C2 crew, and a power supply for the R2C2. The scouts would be dependent on ground troops for force protection. Availability of dedicated troops to patrol with the scouts may be limited. Scouts could be augmented to scheduled patrols to mitigate this problem; however, mission objectives for the patrols and the scouts may be conflicting and difficult to coordinate. Power will be the largest factor of the three previously listed. With access to a stable power source, the R2C2can sustain unlimited operational time.

Mobility of the scouts will be an issue that will extend the timeline of operations. Even though it has been deemed secure, tactical measures still need to be adhered to when moving about the city of Shirāz. Having to physically upload imagery from the field back to the R2C2 will require more time. The availability of military land transport vehicles, will increase their mobility; however, it is not a guaranteed asset.

2.6.5.3 Assumptions

The largest assumption for this scenario is that ground forces will experience light resistance from Iranian forces in the cities of Būshehr and Shirāz. This enables the ground forces to quickly move up to the city of Shirāz and secure a logistics route to and from the Persian Gulf. Being able to move quickly in securing both cities provides a relatively safe environment for the R2C2 crew to operate in.

A second assumption is that insurgent threats in the cities are not to be expected. The two cities will remain fairly secure for U.S. operations. Any threat of engagements will be with Iranian military forces only.

The third assumption for the deployment is that when integrated with the ground command element, the R2C2 will be provided a power source. A dedicated power supply shall be made available for R2C2 use, enabling continuous operations and support to the RCC and ground forces.

Finally, the last assumption is that Chemical, Biological, and Radiological (CBR) warfare is a viable threat in the area of operations. Iran has been researching and developing biological weapons since the mid-80s with the help of Russian scientists. Observing Operations Desert Storm and Desert Shield has given the Iranian government enough incentive to employ biological weapons as a deterrent.[49] All ground forces, including the R2C2 crew, will be prepared to operate in a CBR environment.

2.7 FEEDBACK FROM THE STAKEHOLDERS

The R2C2 team's primary stakeholder was the DJC2 JPO. Three members from the R2C2 team visited the JPO in March 2006 to discuss the scenarios that were generated. The JPO made a few suggestions, and recommended that the scenarios be slightly modified and that we change one of the scenarios to include the SOUTHCOM area of responsibility (AOR). The El Salvador earthquake scenario is a direct result of the recommendations from the primary stakeholder.

The R2C2 team, after making the modifications to the scenarios and developing a scenario in the SOUTHCOM AOR, forwarded the scenarios to the JPO. The JPO reviewed and validated the scenarios and then forwarded them to representatives of the RCCs to get their feedback. Before using the scenarios to develop requirements, the R2C2 team wanted to ensure that its scenarios were in line with how the RCCs expected to use the R2C2 system. Lt COL Jeffrey Renner, USAF, stated,

> The Contingency Response Group [CRG] could/would deploy for all of the 5 missions you list. We are manned and equipped to be light and lean, so any effort to reduce manpower or equipment airlift requirements without reducing capability are always being explored.[50]

After the responses from the RCCs and requirements offices were collected another of the scenarios was revised again. The Pre-Deployment scenario that involved a covert landing in Tehran, Iran, in which the R2C2 team conducted network warfare to obtain information to pin-point the location of high-level civilian and military leaders,

---

[49] Defense Update News Commentary, "Iran's National Deterrent: Weapons of Mass Destruction Program," http://www.defense-update.com/2004/04/irans-national-deterrent-weapons-of.html, April 2004.

[50] Email response from LtCol Jeffrey Renner, USAF, 86th Air Mobility Squadron, spokesperson for the EUCOM Contingency Response Group, March 2006, office communication.

was considered to be a little out of scope, therefore that scenario was replaced, resulting in the development of the Deployment scenario. The final five scenarios were validated and approved by the DJC2 JPO after the inclusion of the Deployment scenario.

On 21 March 2006, members from the DJC2 JPO came to Monterey, California to attend the R2C2 team's Preliminary Design Review (PDR). The JPO gave much insight during the brief, further increasing the relevance of the work that had been completed. After the brief, the R2C2 team had a one-on-one meeting with the members of the JPO to discuss the remaining steps in the completion of the project. This meeting helped narrow the scope of the project as well as supply the JPO with valuable information to be used in testing the RRK.

2.8 CONCLUSION

Introduced to a potential need for a small, rapidly deployable, C2 system by the DJC2 JPO, the R2C2 team began their research into the utility of such a system. To provide direction and understanding, the characteristics of environment, user, mission, and technology for the R2C2 system were deduced and defined. Drawing on multiple sources, such as lessons learned from Operations Enduring Freedom and Iraqi Freedom, QDR 2006, Joint Publications, and DJC2 documents, the value of an R2C2 became more apparent. Interviews with SMEs added additional importance to the study, which amplified the potential operational gains with an R2C2 system.

Once a better understanding of C2 systems was reached, further research was done to define mission needs. Deriving RRK requirements and additional inputs from SMEs resulted in a defined need for an R2C2. The R2C2 team stated this need as: The RCCs need a deployable, standardized C2 system with a small footprint to be utilized by first responders in Joint, Civilian-Military, and Coalition operations. After a need was identified, capability gaps between current C2 systems and the R2C2 were investigated. The following capability gaps were found:

- Lack of standardized, common, interoperable, and deployable C2 capability to support Joint, Multinational, and Interagency Operations.
- Lack of modular and rapidly reconfigurable design to permit flexible addition of new capabilities.

- Lack of a small system for covert intelligence gathering and data transmission.

To help further facilitate the usefulness of the R2C2, identification of the stakeholders was completed. The DJC2 JPO was the project's primary stakeholder as the entity responsible for the development of the RRK. EUCOM, SOUTHCOM, PACOM, CENTCOM, and NORTHCOM were the users of the R2C2 system and their input provided the most value. Additional NPS stakeholders in TNT, COASTS, and HFN were added in recognition of their support and collaborative efforts.

The next step involved determining what types of scenarios to use. Under the guidelines of the Doctrine for Joint Operations, the range of military operations of War and MOOTW was analyzed. A scenario stress matrix was developed using the range of operations and considerations that fall under the three stress points. The scenarios that were chosen included: Pandemic (avian flu in Singapore), Disaster Relief (earthquake in San Salvador), Counterterrorism (southern Philippines), Civil Unrest (Ivory Coast NEO), and Deployment (Iran conflict). These five scenarios were analyzed in the scenario stress matrix to quantify the amount of stress that would be put on the R2C2 in each scenario. This information helped determine the optimum architecture of the R2C2.

The iterative phase of mission analysis conducted by the R2C2 team involved the preliminary background and foundation for the subsequent analysis. This portion of the team's SE process provided justification for the use of an R2C2. The team was able to identify the need for the R2C2 and then elaborated on that by analyzing the system in various scenarios. Supported by feedback from the stakeholders, the R2C2 team reached the mission analysis goal of evaluating the R2C2 in operational scenarios. Established in a clear direction, the R2C2 team moved forward to define requirements based on products completed during the mission analysis phase.

THIS PAGE INTENTIONALLY LEFT BLANK

3.0 REQUIREMENTS

3.1 INTRODUCTION

The requirements generation aspect of the project occurred during the Conceptual Design Phase of the Systems Engineering Process. Upon completion of the mission analysis, operational requirements were generated, utilizing the information obtained from the five scenarios. Operational requirements were decomposed into system requirements after completing the functional analysis and scenario timelines. Both the operational and system requirements laid the foundation for the remainder of the project. The Architecture group designed the system based on requirements and the Modeling and Analysis groups focused on developing models to determine if the architectures met the requirements. This chapter identifies the processes used to develop and refine requirements and compares the R2C2 team-generated requirements to the requirements outlined by the DJC2 CPD and the BAA.

This phase required continuous communications between the R2C2 team and the customer, stakeholders, and SMEs to ensure that all of the user's needs were captured in the generated requirements and were realistic. The R2C2 team contacted people from the Navy Requirements Office (N71C1), JFCOM Requirements Office (J88), EUCOM, PACOM, and CENTCOM, to collect information about potential missions and user's needs in order to help refine requirements that were based on the five scenarios.

Developing requirements did not come without its set of challenges. The most important part about developing requirements was to communicate on a frequent basis with the users, and our short project schedule and the difficulties in identifying the actual operators of the system made this process difficult. Many potential customers who have the most experience with C2 systems and operations were more focused on dealing with real world situations in their Area of Responsibility (AOR) instead of providing input for the development of the system because of its higher priority. Since it was difficult to contact the customers to determine their expected uses and functionality, the R2C2 team composed several scenarios and timelines that covered the range of military operations

(e.g., Pandemic, Disaster Relief, Counterterrorism, War, and Civil Unrest) and formulated a list of requirements.

Before the R2C2 team generated requirements, DJC2 JPO published a CPD and a BAA that listed a number of requirements for the RRK. The CPD and BAA documents do not specify what missions the RRK will be used for or what tasks the RRK must accomplish. The R2C2 team wanted to be able to trace requirements back to the specific tasks identified in a mission, so they developed the scenarios and functional analysis to help justify each requirement. Scenario timelines were developed to place constraints on the system and to develop performance requirements for the R2C2 system. The requirements that were generated by the R2C2 team were then compared to the requirements received from the DCJ2 JPO in the CPD and the BAA.

3.2 TIMELINES

After developing the five scenarios, and vetting them through the customers and stakeholders, the R2C2 team further dissected the scenarios and developed timelines to determine the operational requirements, functional requirements, and system requirements. The timelines helped determine answers to critical questions such as:

- how long does the system need to provide power?;
- what bandwidth is required by the system?;
- what is the range at which data has to be passed?; and
- what is the frequency of data transmissions?, etc.

The following are the five timelines used to generate performance requirements.

Pandemic Timeline

0+00	PACOM receives reports of an outbreak of avian flu in Singapore suspected to be caused by a new strain of H5N1 virus that is capable of spreading among humans
0+10	PACOM makes initial assessment of severity, possible scope of outbreak, and assistance required
0+50	PACOM activates R2C2 crew to configure R2C2 system to gather on-site outbreak information and provide assistance in coordinating medical assistance efforts
1+00	PACOM configures R2C2 system for mission requiring long haul communications, local communications, information management

	system, video or digital camera, maps, virus test kits, and medical software modules
6+00	R2C2 crew departs
12+00	R2C2 crew arrives at Singapore airport
13+00	R2C2 crew arrives at hotel and begins to set up R2C2
13+20	R2C2 crew conducts voice and data checks with PACOM and with organic communications and sensors via R2C2 system
13+30	Medical scouts dispatched to gather information from U.S. Embassy and local authorities via R2C2 system
16+00	R2C2 crew sends initial reports on virus information, scope of outbreak, and containment actions by local authorities
22+00	Medical scouts collect samples of virus and digital imagery from local health facilities. R2C2 crew sends images back to RCC via R2C2 system
+1 day	R2C2 conducts video teleconference (VTC) once a day with RCC to support telemedicine consultation Constant exchange of messages throughout the day to coordinate medical tests and results Upload of digital signature of virus result images every four hours Exchange of coordination information on further medical assistance of ESG Collaborate with other NGOs on-site Coordinate and track movement of medical scouts as they go about gathering information and rendering assistance Keep track of the spread of virus
+ 3 days	R2C2 establish connectivity with ESG Coordinates prearrival arrangements

Disaster Relief Timeline

0+00	SOUTHCOM receives reports of major earthquake in Central America
0+10	SOUTHCOM unable to contact Forward Operating Base and Embassy
0+50	SOUTHCOM alerts R2C2 crew
1+00	SOUTHCOM configures R2C2 system to include long haul communications, local communications, information management system, video or digital camera, maps, firearms, and translation software
6+00	R2C2 crew departs RCC via helicopter
12+00	R2C2 crew arrives at airport
12+20	R2C2 crew finds U.S. staging area and personnel begin to set up R2C2
13+00	R2C2 crew conducts voice and data checks with SOUTHCOM and with organic communications and sensors
13+30	R2C2 crew sends video clips of the coastline and airfield taken while onboard helicopter to SOUTHCOM

15+00 R2C2 reports that U.S. military personnel accounted for at airport with minor first aid needs

20+00 R2C2 scouts find rides with local military to embassy, fairgrounds, and Acajutla Port

22+00 Scouts give on-station report to R2C2 crew

+1 day Scouts give hourly reports
From the port, the scouts report damage and security issues: is it suitable to receive shipments from ESG and other relief ships?; are roads from port to San Salvador open?; is it safe to operate?
From the Embassy, the scouts report the status of U.S. personnel and medical requirements
From the fairgrounds, the scouts report status of creating a CMOC with local government, IOs, and NGOs
R2C2 relays port and landing zone data to ESG (pictures/voice) and RCC
R2C2 receives satellite imagery from RCC and shares information with the CMOC
FOB provide mobile generators for power

+ 5 days ESG arrives
Scouts pass bihourly reports to R2C2
R2C2 compiles reports and passes status to SOUTHCOM and ESG
R2C2 crew relays evacuation data between CMOC and ESG
R2C2 relays CMOC needs for medical, water, and equipment to SOUTHCOM and ESG
R2C2 operations continue until some local communications have been restored

Counterterrorism Timeline

–30 days United States and Republic of the Philippines forces conducting Balikatan training/exercises on nearby island of Basilan with the aid of an R2C2 system

0+00 U.S. receives intelligence of increased Abu Sayyaf activity; the possibility of a terrorist attack in Manila; and that a high ranking al-Qaeda leader is temporarily in camp near the town of Buriasan

1+10 Intelligence report is passed to Filipino government with request to immediately utilize SOF to locate terrorist camp before al-Qaeda leader departs area within the next 24 hours, and pass streaming video of high ranking al-Qaeda leader to U.S.

2+00 Intelligence report and mission is passed to U.S.-RP forces conducting training in Basilan

2+30 U.S.-RP forces (8-man team) halt training and prepare to move to Mindanao Island, along with R2C2 system

5+30	U.S.-RP forces arrive on Mindanao Island to conduct counterterrorism operation
6+30	RP forces initiate surveillance in and around Buriasan to obtain information as to location of terrorist camp and al-Qaeda leader
8+30	U.S.-RP concludes initial surveillance in and around Buriasan and covertly moves to location from which to conduct mission
11+30	R2C2 site determined
12+00	R2C2 is set up and attains positive communications and data checks with RCC and organic sensors
12+00	Initial SITREP sent from R2C2 to RCC
12+15	Scouts deployed to covertly locate terrorist training site. Information will be gathered through field PDAs/cameras/camcorders/radios and transmitted to R2C2
15+15	Terrorist camp located and surrounded
16+20	Video of terrorist camp passed to R2C2
16+25	Video relayed to RCC
18+00	Streaming video of possible high level terrorist leader sent to R2C2
18+05	Streaming video relayed from R2C2 to RCC
20+14	Order to strike terrorist camp is issued
20+18	Order received by R2C2
20+19	Order passed to organic sensors
20+42	Simultaneous attack on terrorist camp initiated to take out terrorists and high level leader

Civil Unrest Timeline

–5 days	EUCOM receives report that rebel forces have increased attacks on UN/French troops in Ivory Coast
–4 days	EUCOM alerts ESG leaving Strait of Gibraltar toward Norfolk, Virginia and redirects them to make best speed (18 kts) toward Ivory Coast to conduct possible NEO
0+00	EUCOM receives distress call from U.S. Embassy in Abidjan for an assisted evacuation of American citizens
0+30	EUCOM alerts two R2C2 crews
0+45	EUCOM configures R2C2 systems to include long haul communications, local communications, video and digital cameras, movement sensors (infrared (IR), acoustic, visual), maps, translator, and firearms
1+00	Embassy orders all U.S. citizens to report to the U.S. Embassy
5+00	R2C2 crews deploy via commercial aircraft
11+00	R2C2 crews arrives Abidjan International Airport
11+20	R2C2 crews locate U.S. personnel from Embassy and depart for mission areas (Crew A: Embassy; Crew B: Yamoussoukro)
11+35	Crew A arrives U.S. Embassy and begins R2C2 set up
11+55	Crew A establishes reachback link

12+00	Crew A conducts voice and data check with EUCOM, en route ESG, NGOs, organic communications, and sensors
12+05	Crew A coordinates with Embassy over preplanned evacuation plan
12+10	Crew A deploys scouts to take visual pictures of landing site for helicopter evacuation
12+30	Crew A sends SITREP with ESG Embassy evacuation plan and imagery of landing site
13+20	Crew B arrives in Yamoussoukro at French/UN command position and begins set up of R2C2 system
13+30	Crew A reports hourly SITREP
13+55	Crew B conducts voice and data check with Crew A, EUCOM, ESG, UN troops, French troops, organic communications and sensors
14+00	Crew A receives initial tasking from Marine Expeditionary Unit Commander for NEO
14+05	Crew B deploys scouts with French escorts to set up motion sensors
14+15	Crew B relays initial SITREP to EUCOM, ESG, and Crew A of information gathered from French/UN command
14+20	Crew B receives satellite imagery from EUCOM displaying concentration of rebel forces and unclassified (UNCLASS) imagery is shared with UN/French
14+30	Crew A reports hourly SITREP
15+00	Crew B scouts report sensors in place. Scouts move to take video imagery of any rebel activity. R2C2 begins collecting data from motion sensors
15+15	Crew B reports hourly SITREP to Crew A with available data collected by sensors and video imagery from scouts
15+30	Crew A reports hourly SITREP
16+15	Crew B sends SITREP
16+30	Crew A reports hourly SITREP with evacuee information to ESG commander
17+15	Crew B reports SITREP showing a halt in advancement, but a buildup of rebel forces on the outskirts of Yamoussoukro
17+15	Hourly SITREPS by both crews
20+30	Crew B reports start of rebel movement and increase in fighting
21+00	Crew B breaks down R2C2 system and extracts from Yamoussoukro back to Abidjan via French transport
23+00	Crew A reports weather conditions, confirms safe landing zone, and confirms estimated time of arrival (ETA) with ESG commander
23+15	Crew B arrives at the U.S. Embassy
24+00	ESG arrives on station ESG deploys helicopters to evacuate U.S. citizens and R2C2 crews from Embassy. Crew A breaks down R2C2 system when all U.S. citizens are safely evacuated

Deployment Scenario Timeline

–6 days	U.S. ground forces enter Iran and begin conflict
–4 days	U.S. forces secure city of Būshehr
–1 days	U.S. forces secure city of Shirāz
0+00	R2C2 crew enters Iran
2+00	R2C2 crew arrives at Shirāz and joins ground command element
2+30	R2C2 crew establishes reachback with CENTCOM
2+45	R2C2 crew conducts voice and data checks with CENTCOM, ground forces, and organic communications and sensors
3+00	R2C2 scouts deploy into city of Shirāz
3+00	R2C2 crew reports to CENTCOM with initial information of force status, environmental issues, general SA
3+20	R2C2 crew receives imagery from RCC of possible pockets of resistance, updated city map, Iranian force movement in the vicinity
3+25	R2C2 crew passes information to ground command element
3+45	R2C2 crew receives reports from scouts
4+00	R2C2 crew reports SITREP with imagery of local population and initial BDA of the city
4+45	R2C2 crew receives imagery from RCC with updated ppposition forces information
4+45	R2C2 crew receives reports from scouts
4+55	R2C2 crew passes CENTCOM information to ground command element
5+00	R2C2 crew reports SITREP to CENTCOM with imagery of potential locations for DJC2 staging
5+10	R2C2 crew passes same information to construction battalion
5+30	R2C2 crew receive updated imagery from RCC
5+40	R2C2 crew passes imagery to command element
5+45	R2C2 crew receives updates from scouts
6+00	R2C2 crew reports STIREP CENTCOM with amplifying information on previously reported staging areas (infrastructure, size dimensions, accessibility, protection, habitability, etc.)
6+15	R2C2 crew passes same information to construction battalion
6+45	R2C2 crew receives reports from scouts
7+00	R2C2 crew reports SITREP with additional staging areas and amplifying BDA
7+10	R2C2 crew passes additional staging areas to construction battalion
7+45	R2C2 crew receives reports from scouts
8+00	R2C2 crew reports SITREP with amplifying information on staging areas
8+15	R2C2 crew passes same information to construction battalion
12+00	RCC crew tells R2C2 crew choice for DJC2 staging area
12+10	R2C2 scouts are redirected to chosen area for further evaluation
12+15	R2C2 crew passes chosen site to construction battalion and ground command element

14+00	R2C2 crew receives additional imagery and information on staging area
14+15	R2C2 crew passes information to construction battalion
+4 days	Initial elements of DJC2 arrive in Shirāz

3.3 OPERATIONAL REQUIREMENTS

Operational requirements outlined the capabilities needed by the system to complete the intended mission. They do not specify how these capabilities must be met. To determine the capabilities required of the system, the R2C2 team had to realistically answer the following crucial questions:

- what functions will the system perform?;
- when will the system be required to perform its intended functions and for how long?;
- where will the system be used?; and
- how will the system accomplish its objective?

Answering the above questions provided insight as to how the system will be used and function. Once the intended uses and functions of the system were determined, it was feasible to start thinking of ways to develop a new system or simply locate a COTS system that already has the ability to perform the intended functions. After determining the functions of the system, figuring out when the system would be required to perform those functions and for how long was one of the driving factors behind the development of timelines. By calculating when the system would have to operate and for what durations, the R2C2 team determined organic power duration requirements for the system if local power was not available. Deciding in what environments the system would operate generated many questions:

- how to protect the system in excessive weather conditions?;
- how to protect the system in extreme heat?;
- how to power the system if local power is not available, how to protect electronic components in dusty areas?; and
- how to secure the system in hostile locations?

Answering the question, how will the system accomplish its objective? required the team to look at different types of software and hardware components. If the mission

required only voice transmissions, determining the required components was relatively simple, but if the mission required streaming video transmissions, then that operational requirement placed more stress on the system by requiring higher bandwidths, more power, and additional wireless components to relay information back securely to the Primary Suite. The ability to provide local communications, within 35 miles of the Primary Suite, and long haul global communications were essential in order to better facilitate gathering, processing, and passing information to the required entities.

The evaluated missions required classified information transmission that, if placed in the wrong hands, could not only jeopardize the mission, but possibly endanger the lives of those conducting the mission. This drove the requirement to provide a secure means of passing and receiving operational and tactical information to and from the supported commander. Not only does the information need to be secure, but the equipment being used and the personnel operating that equipment must also be trusted—driving the need for physical, data, and network security. In some scenarios, the R2C2 will be operating in a hostile environment that added the requirement to protect the physical location of the equipment, secure access to the equipment, secure access to the room or location where the equipment will be staged, and secure the identity of the personnel that are out in the field collecting data for the R2C2.

Working with organizations outside of the U.S. military introduces many variables when determining R2C2 concepts of operations and requirements. When working with agencies that are not a part of the R2C2 system, such as IOs, interagencies, NGOs, and local government agencies, establishing ways to transmit information was difficult. Almost all agencies use different communications systems and frequencies, requiring the R2C2 system to be interoperable with many other entities. The ability to share data and information was one of the most important aspects to effectively work with other organizations, as well as one of the most challenging. Not only does the R2C2 system need to share information with coalition or a civilian authorities, it needs to transmit and receive critical information to and from the scouts.

Power was one of the most important constraints for any contingency response operation. Most of the scenarios were in austere locations where no local power was available and required the R2C2 system to provide organic power, such as batteries or

generators, until the local power could (if possible) be restored. Bringing along generators was a viable option for some scenarios (i.e., Deployment, Pandemic, Natural Disaster), but not for the Civil Unrest and Counterterrorism scenarios, due to the high probability of being detected if a generator was used in those situations. Thus, these two particular scenarios required the use of battery power. Additionally, if power is available, the R2C2 system must be equipped with power adapters or conversion devices.

The scenarios and timelines evaluated required the use of scouts to supply time-critical information essential to mission completion and success. In order for them to provide the R2C2 with situational awareness, the scouts needed to collect and display data and transmit information back to the R2C2 system. The R2C2 operators also needed a means by which to collect and display the data that was transmitted from the scouts. After receiving data from the scouts, the R2C2 operators have to analyze, compile, and pass the data to the RCC.

This system will be carried to some of the most austere locations depending on the mission, requiring that the delicate electronics be packaged properly to sustain the jarring that may be encountered during transport. Since the system must be mobile and ready to go on short notice, the packaging must withstand the vibrations and pounding customary onboard naval aircraft, ships, and land vehicles. The ability to transport the R2C2 system via commercial aircraft dictates the size and weight of the system as well as the packaging of the system.

The expectations of the R2C2 system to have a small footprint and be able to complete a wide range of missions required the system to be adaptable and flexible to fulfill any mission. The system has to be able to switch from a humanitarian mission to a counterterrorism mission with very little added stress to the operator, requiring that the system have software and hardware connections to facilitate the addition of new mission modules.

The following are the operational requirements that the R2C2 team derived from the scenarios.

(1) Provide capability of local and long haul communications to the RCC, DJC2, other R2C2 systems, coalition partners, military assets, and civilian assets.

(2) Provide secure means (physical security, data security, and network security) of passing tactical information to the supported commander for SA.

(3) Provide means of collecting data from organic or inorganic assets.

(4) Provide self-supporting power supply in addition to the capacity to operate on standard electrical power.

(5) Provide capability for operators to receive, display, analyze, filter, and pass simultaneous data from organic or inorganic assets.

(6) Provide compact, rugged, and mobile packaging

(7) Provide flexibility for mission-dependent software and hardware configurations.

3.4 SYSTEM REQUIREMENTS

System requirements describe what the system must do, but not how the system should do it in regard to specific hardware, software, facilities, people, or data.[51] Determining the system requirements for the R2C2 system was an iterative process. The R2C2 team analyzed the scenarios and timelines to identify performance requirements necessary for mission success. The R2C2 team focused on the six primary requirement areas to determine requirements:

- BW (for both local and long haul communications);
- security (physical, data and network);
- data types (streaming video, images, video, and voice);
- power (amount needed and duration);
- information management; and
- weight.

By identifying the scenarios that placed the greatest strain on the system, it was possible to further determine the minimum performance capabilities of the system to operate in all five missions.

---

[51] B.S. Blanchard and W.J. Fabrycky, *Systems Engineering and Analysis*, 3rd Edition, Prentice Hall, 1998, pp. 48-50.

The BW requirements were calculated by analyzing the timelines to determine what type of data and how often the information would be transmitted to and from the inorganic and organic sources in the local area or outside of the operating area. The analysis of each scenario was critical in determining the minimum amount of BW that would be needed to perform each mission for local and long haul communications. Factors that played heavily in determining the BW requirements were:

- how much data would be transferred?;
- what type of data would be transferred (voice, images, video or streaming video)?;
- how often would that data be transferred?;
- in what type of environment would that the information be passed?, and
- how much security would be needed to ensure that sensitive information arrived at its intended destination without being compromised?

Security also placed restraints on the system and involved the protection of the actual location of the R2C2 system, the data being passed to and from the system, and the network on which the R2C2 system was operating. Some of the scenario locations were hostile, requiring physical security to prevent anyone from entering the room where the system was being operated, in an attempt to destroy, gain access to, or monitor the system. This requirement increased the number of people operating the system (from 2 to 4) in order to provide security as a safety measure. Securing the data required encryption, biometrics, or authentication to gain access to a device in order to input information or pass that information to the R2C2. Network security required that information being passed was encrypted and that the network be protected from hackers gaining access to sensitive information that could jeopardize the mission.

Based on the scenarios, the types of data that needed to be transmitted ranged from voice only, to images, to streaming video. The BW requirement for a voice only transmission was small in comparison to the streaming video bandwidth requirement. Not only is the streaming video BW requirement high, the amount of power needed to transmit was affected.

The power required for each mission was calculated from the amount and type of data being passed and the frequency of that data transmission. Some scenarios (e.g., the

Pandemic) would require a lot of information to be passed, especially early in the mission in order to gain a complete assessment of the severity of the outbreak. The amount of information that would be passed and the relatively frequent requirement for passing that information necessitated a high demand for power. The power requirement also takes into account the number of people who would be using the system to access information to the Internet or other organization's databases such as the WHO or the Red Cross.

The length of time that power would be required was determined by analyzing the scenario timelines and looking realistically at how long the system would be in operation before commercial power was available. Some scenarios lacked local power, requiring the system to provide its own power. The longer the system has to operate without commercial power, the more restrictive the organic requirement became. If the scenario was in a location that was destroyed by natural forces, the entire scenario required the use of a mobile power source. If local power was available, the duration of organic power was minimized, depending on the reliability of the local power grid. The R2C2 team determined that the system primary suite will consume approximately 1,350 watts of power. The local power grid must be able to support this power consumption in order for the organic power supply requirement to be reduced.

The management of information included the means by which the R2C2 crew analyzed, displayed, edited, and entered information. The more interactions the system had with the information, the higher the requirement for information management. These interactions were classified into the following categories: data input (keyboard, point devices, floppy disk drive, Ethernet port, wireless local area network (LAN) interface, speakers, headphones, or camera for video conferencing), data storage (hard disk, secondary storage, Universal Serial Bus (USB) thumb drive for data exchange with external parties), data analysis (messaging software, Web browser, mission planning software, blue force and enemy tracking software), data presentation (color Liquid Crystal Display (LCD) screens, printers, scanners, or projectors), and data protection (antivirus software, encryption software, and access control mechanism such as Common Access Card (CAC), secure token or biometric). As the data received by R2C2 system increased, the more information management became important to extract and compile information to develop the situation awareness picture for the RCC.

The R2C2 system will be a mobile system that must be transported by two personnel. This restriction placed constraints on the weight of the system. It must be commercial airline checkable, which further restricted the weight and size of the system. The weight of the system can vary depending on its mission and mode of transportation. The commercial restrictions for luggage is 40 pounds for carryon and 70 pounds for checked luggage and the military restrictions for luggage is 45% of the operator's weight. If the system is being carried by military means, the weight can be higher, especially if it does not have to be carried by two people once it gets into the operating area.

Table 4 shows the break out of the system requirements for all five scenarios (Pandemic, Disaster Relief, Counterterrorism, Civil Unrest, and Deployment). The six primary requirement elements were rated against the scenarios to determine which scenario placed the greatest amount of stress on the system, so that if only one system was designed, the system would meet the requirements for all missions. The matrix is interpreted as follows: red indicates a higher requirement, leading to a more stressful situation for the R2C2 system, green is low stress on the system, and yellow is moderate stress on the system. The legend at the bottom of Table 4 explains what is considered to be high, moderate, and low stress for each of the six requirement elements.

	Pandemic	Disaster Relief	Counter Terrorism	Civil Unrest	Deployment
Bandwidth (local)					
Bandwidth (long haul)					
Security					
Data Types					
Power (Required)					
Power (Duration)					
Information Management					
Weight					

Legend	Bandwidth	Security	Data Types	Power (Required)	Power (Duration)	Information Management	Weight
	>2 Mbps	Physical, Data & Network	Streaming Video	High	> 24 Hrs	High	>90
	1-2 Mbps	Data & Network	Video & Images	Medium	12-24 Hrs	Medium	70-90
	<1 Mbps	Data	Voice	Low	< 12 Hrs	Low	<70

Table 4: Operational Requirements

3.5 FUNCTIONAL ANALYSIS

> Functional analysis is the process of translating system requirements into detailed design criteria, along with the identification of specific resource requirements at the subsystem level and below. One starts with an abstraction of the needs of the customer and works down to identify the requirements for hardware, software, people, facilities, data, or combination thereof.[52]

By looking at the functions that the system must fulfill according to the scenario, timelines, and customer needs, the R2C2 team dissected those functions to determine specific requirements of the system. In order to generate the functional requirements of the R2C2 system, the R2C2 team used two different approaches. The first approach was to look at the R2C2 system from the operators' point of view by developing a Functional Flow, to ensure that all user requirements were taken into account and the second approach was looking at the R2C2 system from a mission point of view by developing a

[52] B.S. Blanchard and W.J. Fabrycky, *Systems Engineering and Analysis*, 3rd Edition, Prentice Hall, 1998, pp. 62-63.

Functional Tree. Both aspects provided insightful information in the development of requirements for the R2C2 system.

3.5.1 Functional Flow

The Functional Flow analysis looked at every aspect of the R2C2 system, from getting the team together, deploying with the system, completing the mission, and reconstituting the R2C2 system. The Functional Flow divided the operation of the R2C2 system into three categories: deploy, conduct mission, and reconstitute. These three operations were further divided into more categories until actual requirements of the system were reached.

The deployment section of the analysis required looking at the time to marshal the system, transport the system, and setup the system making it operational. Marshalling the system required assembling the team, selecting the proper components for the mission, packaging the system based on the type of environment it would have to endure, and loading the system on a transport vehicle. Transporting the system was broken into three categories depending on how the system would be deployed: by air, sea, or land. Once the system was transported to its operating location, it required a timely set-up. The set-up involved determining the optimum location for system operations, establishing means by which to power the system (commercial or mobile), and finally, conducting system checks to ensure the system was fully operational to conduct the intended mission.

Conducting the mission included the majority of the R2C2 system functions. The most stringent requirements were generated from this part of the Functional Flow analysis. Conduct mission was divided into four categories: provide communications, provide situational awareness, provide situation security and assurance, and provide infrastructure.

Providing communications required communicating both with local links and long haul links. Once it was determined what type of link would be needed, the R2C2 team had to determine who would be communicating. Afterwards, the information was further dissected into three types: video, voice, and data. After analyzing the type

data and frequency at which it was to be transmitted, it was then possible to determine the bandwidth and the best communication link to pass the data to the intended recipient.

SA was the ability of the R2C2 crew to access, modify, and display the collected data. SA required the means to collect data, store data, analyze data, display data, and afterwards output or transmit data to the RCC.

Situational security and assurance (SSA) involved the protection of the R2C2 system as well as those operating it. Physical security, data security, network security, and system availability were required to ensure that the R2C2 system was able to accomplish its intended mission.

Providing power to support ongoing R2C2 operations, providing environmental protection against the elements (dust, heat, etc.), ensuring that logistic support was available for operations, and providing a user interface that allows the operator to interact with the R2C2 system were critical to the infrastructure and required by the R2C2 system.

The reconstitution category focused on the life of the R2C2 system immediately following the completion of a mission. The system would be dealt with in one of the following three ways: integrated with the DJC2, meaning that it would become a part of the DJC2 core infrastructure; redeploy or be reassigned to carry out another mission within the RCC's AOR; or simply exit the theater and return to the RCC without any additional tasking.

The Universal Joint Task List (UJTL) is a ". . . manual that provides a standardized tool for describing requirements for planning, conducting, evaluating and assessing joint and multinational training"[53] written by the Joint Chiefs of Staff (JCS). The UJTL lists an array of requirements that are used to ensure that missions accomplish the goals set forth by the JCS, e.g., the R2C2 team's scenario missions would require the following tasks be met: OP 2.2 Collect and Share Operational Information, SN 2.4.1 Evaluate, Integrate, Analyze, and Interpret Information, and SN 3.3.6.1 Assess Critical Infrastructure (CI) Impacts to Operational Capability, to name a few. The R2C2 team referenced the UJTLs to ensure that the generated requirements were in compliance and

[53] Chairman, Joint Chiefs of Staff Manual 3500.04D Universal Joint Task List (UJTL), 1 August 2005, p. 1.

along the same lines as those outlined by the Joint Staff. The complete Functional Flow analysis and the requirements that were generated from it, along with the associated UJTLs, are found in Appendices C and B.

3.5.2 Functional Tree

The Functional Tree analysis dissected the mission of the R2C2 system from a mission point of view. The form of analysis provided much of the same information as the Functional Flow except it gave more detailed information about the mission specifics. When comparing the two forms of analysis, it became apparent that many of the elements revealed in the Functional Flow analysis were duplicated in the Functional Tree analysis. The Functional Tree Analysis is in Appendix C.

3.6 R2C2 SYSTEM REQUIREMENTS

The requirements below describe the operation of the R2C2 system. It states the minimum performance requirements that must be met by the system in order to successfully complete the assigned mission. The list does not include the type of networks or channels that the R2C2 system must utilize in order to meet the stated requirements.

Deployment

1. Local Communications ≥ 1.8 Mbps (max range 10 miles)
2. Long Haul Communications ≥ 1.8 Mbps
3. Security – Physical, Data, and Network
4. Data Types – Voice, Images, and Video
5. Power Duration – 12 hours
6. Information Management Resources – Medium
7. Weight ≤ 45% body weight per case
8. Size – Two-person transportable

Counterterrorism

1. Local Communications ≥ 2.8 Mbps (max range 5 miles)
2. Long Haul Communications ≥ 2.8 Mbps
3. Security – Physical, Data, and Network
4. Data Types – Voice, Images, Video, and Streaming Video
5. Power Duration – 10.5 hours (darkness)

6. Information Management Resources – Low
7. Weight ≤ 45% body weight per case
8. Size – Two-person transportable

Disaster Relief

1. Local Communications ≥ 2.5 Mbps (max range 35 miles)
2. Long Haul Communications ≥ 2.5 Mbps
3. Security – Physical, Data, and Network
4. Data Types – Voice, Images, and Video
5. Power Duration – 2-8 Weeks (if power is not available)
6. Information Management Resources – High
7. Weight ≤ 45% body weight per case
8. Size – Two-person transportable

Civil Unrest

1. Local Communications ≥ 1.8 Mbps (max range 10 miles)
2. Long Haul Communications ≥ 1.8 Mbps
3. Security – Physical, Data, and Network
4. Data Types – Voice, Images, and Video
5. Power Duration – 11 hours (if power is not available)
6. Information Management Resources – Medium
7. Weight ≤ 45% body weight per case
8. Size – Two-person transportable

Pandemic

1. Local Communications ≥ 2.4 Mbps (max range 20 miles)
2. Long Haul Communications ≥ 2.5 Mbps
3. Security – Physical, Data, and Network
4. Data Types – Voice, Images, and Video
5. Power Duration – 2-8 Weeks (if power is not available)
6. Information Management Resources – High
7. Weight ≤ 45% body weight per case
8. Size – Two-person transportable

3.7 PROGRAM OFFICE CPD AND BAA REQUIREMENTS AND THE DIFFERENCES

The JPO developed two documents that list the requirements for the RRK. The CPD and the BAA stated system requirements for the RRK. These requirements were based on stakeholder inputs and similar systems, and were not necessarily tied to a particular mission or task. Some of the requirements were derived based on the systems

that are currently being used by U.S. military forces. The CPD requirements that were determined to be critical are:

- Agile, quick response capability with small footprint
- Satellite connectivity designed to serve up to four operators
- Expandable to up to ten in group collaboration with reachback to Internet, NIPRNET, SIPRNET, and required multinational/coalition networks and collaboration tools and services
- Transportable on commercial or military aircraft
- Transportable by 2 persons
- Operable on standard electrical power sources
- Capable of operating on small lightweight organic power sources such as host national power grid, facility power or generators
- Operable in austere locations
- Provide data and voice communications and collaborative capabilities via reachback
- Provide limited capability to include SHF, SATCOM, UHF, TACSAT, INMARSATA, and handheld global satellite phone for SA, planning and other C2 functions[54]

The BAA requirements that were determined critical are listed below:

- Provide capability to connect to two (2) GIG-accessible, crypto-covered networks at once (e.g., NIPRNet, SIPRNet, CENTRIXS)
- Provide secure wireless (objective) to clients
- Utilize Everything over Internet Protocol (EoIP)
- All equipment must meet commercial standards for carry-on luggage for commercial aircraft (Objective: Transport by two persons)
- Provide Net Centric operations to the maximum extent possible
- Demonstrate multi-mode (data, video, and voice) operations
- Provide minimum of four (4) Voice over IP (VoIP) telephonic instruments and four (4) client computers

[54] DJC2, CPD, OPNAV N71C2- 688(1)-71-05, 30 November 2005, pp. 19-21.

- Must be able to use thin or thick clients, and must support 5 clients (threshold)/15 clients (objective)
- Provide radio with 1.024 Mbps threshold, 4.196 Mbps objective per network
- Provide reliability, maintainability, availability, built-in test and logistic support as an objective
- Provide compact, ruggedized, protective packaging[55]

Though the basic requirements in the CPD and the BAA are comparable, the differences posed a new set of problems for the R2C2 team. Both documents do state the need for a lightweight system that is two-person transportable, but the CPD states a need for up to ten operators and the BAA states a need for 5-15. Determining which set of requirements, or which particular requirement, was most important, if two requirements were contradictory, gave the R2C2 team the flexibility to determine which requirement to use based on mission analysis.

3.8 DIFFERENCE BETWEEN JPO REQUIREMENT AND R2C2 TEAM REQUIREMENTS

During the analysis of the missions and timelines, the R2C2 team developed similar operational requirements for the system as the JPO and identified the need for additional capabilities to be mission effective. Some of the differences impacted the amount of equipment and the weight of the system. The fully operational R2C2 system does not meet the two-person transportable requirement outlined in the CPD and BAA for a RRK. This is due to additional capability that the R2C2 teams deem necessary to successfully develop SA. The additional capability includes the Local and Civilian/Military Suites that allow scouts, civilian, and military agencies to utilize the R2C2 system's capabilities. The Local Suite was designed to give a "data link" to the scouts to improve the transmission time of relevant information to the Primary Suite (the central operating hub for the R2C2 system). The Civil/Military Suite was designed to

[55] Joint Program Office, Broad Area Announcement for Rapid Response Kit, FBO: DON-SNOTE-05-0624-002, Version 2.0, p. 4.

give NGOs and Private Voluntary Organizations (PVOs) access to the internet to facilitate reachback to databases and other agencies not in the region for HA/DR.

The R2C2 team determined that the system needed an organic power supply since 60% of the evaluated scenarios did not have local power available. The CPD stated that the system needs to be "capable of operating on small lightweight organic power sources such as host national power grid, facility power or generators,"[56] the R2C2 team took this requirement a step further, making the power source a part of the R2C2 system. Based on the scenarios and timelines, it became apparent that the locations in which the R2C2 system would operate may only have intermittent power and self-supporting power would have to be transported with the system.

The task of the R2C2 team was to develop a set of requirements that could be tied to specific missions in order to add validity to the requirement. Because of this task, some of the requirements that were developed by the R2C2 team were not part of the requirements captured by the JPO. In order to provide a system architecture that fulfilled the needs of the JPO, their requirements were analyzed and incorporated if they traced back to mission tasks.

3.9 FEEDBACK FROM STAKEHOLDERS

The feedback received from the JPO was very constructive. Their feedback allowed the R2C2 team to focus their efforts on particular aspects of the project that minimized risk and allowed the R2C2 team to complete the project in the allotted time. The JPO made the suggestion that the R2C2 team focus only on voice communications links from the organic sources to the R2C2 crew.

3.10 CONCLUSIONS

The development of requirements involved many different analysis methods. Analyzing the scenarios and timeline to determine requirements, with the feedback from the JPO and customers, ensured that the requirements were relevant and realistic. After the development of the timelines, the operational requirements and system requirements

[56] DJC2, CPP, OPNAV N71C2-688(1)-71-05, 30 November 2005, p. 20.

were derived. The construction of the Functional Flow and Functional Tree allowed the R2C2 team to dissect operator and system tasks to determine all functions that the system had to fulfill. Some of the scenario- and timeline-based system requirements generated by the R2C2 team differed from the list that the JPO promulgated. The difference in requirements made the process a little difficult when deciding which requirements were the most important. The R2C2 team mitigated the difference in requirements by evaluating all requirements set forth by the CPD, BAA, and R2C2 team to see if each requirement could be traced to a specific mission task. The final requirements were compared to the UJTLs to determine if the system requirements were consistent with those requirements established by the JCS. Most of the requirements generated for the R2C2 system were in compliance with those listed in the UJTLs, adding validity to the R2C2 team's requirements. The completion of the requirements made way for architecture construction and modeling.

THIS PAGE INTENTIONALLY LEFT BLANK

4.0 SYSTEM ARCHITECTURE DESIGN

4.1 INTRODUCTION

System architecture design is a part of the SE process that relates system functional requirements to physical system design. The architecture describes a relationship between products, requirements, and overall system interaction. The system architecture design for the R2C2 was completed at a top level of abstraction. All system designs were completed through the use of scenarios, functional flow, requirements mapping, and user input. Given the wide range of scenarios and required functionality, the R2C2 system was broken down into different suites that offer differing functionality, flexibility, and scalability. The R2C2 system consists of three suites: the Primary Suite (PS), the Local Suite (LS), and the Civil/Military Suite (CMS). One PS, three LS alternatives, and two CMS design alternatives were selected for modeling and evaluation.

This chapter covers the approach used to identify different design architectures, trade-offs, and final design. Additionally, any assumptions that were made during the course of the design were outlined in each respective section.

4.2 APPROACH

The first steps taken in the design of the R2C2 system were to identify all communication links needed in each scenario, develop a system design template called the Architecture Baseline, and identify current technology and software maturity through a market survey. These three phases of approach led to the generation of multiple alternatives as well as the creation of the R2C2 suites.

4.2.1 Communication Link Identification

The communications necessary for each scenario were analyzed using the previously generated timelines and CONOPS. Table 5 shows all of the different communication links identified. A green box denotes the need for that particular type of communication capability, while a red box denotes that no communication link between the entities was required.

	Civilian Communication		Tactical Communication	Coalition Communication		Strategic Communication
	Local	Long Haul	Local	Local	Long Haul	Long Haul
Disaster Relief						
Pandemic						
Civil Unrest						
Counterterrorism						
Deployment						

Table 5: Communication Links Needed in the Scenarios (green means the link is needed)

The civilian communication link represented local or long haul communication. Local civilian communication was a connection with local authorities, NGOs, IOs, etc., within the area of operation. Long haul civilian communication was the link back to civilian resources and databases outside the area of operation. Tactical communication represented communication with the R2C2 scouts who were within the area of operation collecting data and intelligence. The coalition communication link was either via a local link or via the CENTRIXS link. The CENTRIXS network facilitates multinational information sharing by combining many different global networks in a common, virtual location.[57] In order to access CENTRIXS, a user must have a long haul connection to the Global Information Grid (GIG) and the SIPRNET. The GIG is classified as a data computing grid that connects all Department of Defense technologies and users via networks like SIPRNET and the NIPRNET. Lastly, the strategic link was a connection back to the RCC and/or to the GIG for NIPRNET, SIPRNET, and CENTRIXS access.

In the Disaster Relief and Pandemic scenarios, civilian, tactical, and strategic coordination was needed; specifically, an emphasis was placed on civilian coordination to help in quick response, aid, and information collection. As shown in Table 5, the Civil Unrest scenario required the R2C2 to be connected to all communication contacts. Civilian, tactical, coalition, and strategic communications capabilities were needed for proper mission execution. Lastly, both the Counterterrorism and Deployment scenarios displayed a need for a streamlined R2C2 system to reduce the system footprint. These scenarios did not require a civilian or coalition communication capability.

Upon further investigation into the requirements for each of the four communication types, the R2C2 team determined that each had required functions as well

[57] The Joint Interoperability Test Command, "Combined Enterprise Regional Information Exchange System (CENTRIXS)," http://jitic.fhu.disa.mil/washops/jtca/centrix.html. Last accessed in May 2006.

as a potential for enhancement to improve link capacity. For civilian communication, a local voice link as well as a long haul data link back to civilian databases and resources were required. An enhancement to the civilian communication system was determined to be the addition of an Internet access point for limited civilian use. This conclusion was based on user input and HA/DR findings in the previous chapters. For the tactical communications link, it was concluded that voice communications would be sufficient to pass important information. However, adding a wireless, long-range connection could increase SA for the R2C2 operators by providing scouts the means to transfer video and data in real time. The coalition communication link must simply ensure a voice and CENTRIXS capability. No enhancements to this communications link were identified. Lastly, the strategic communications link provided R2C2 operators the ability to send voice, video, and data. This requirement came directly from mission analysis as well as both the DJC2 CPD and BAA documents. To enhance the long haul link, a high bandwidth satellite terminal must be teamed with a high bandwidth satellite constellation.

The identification and elaboration of all the links needed for communication required the R2C2 team to further investigate communications links not specified in the DJC2 CPD and BAA. Both the civilian communication enhancement and the tactical link were not addressed by the CPD and BAA, but have been deemed necessary given the previous mission analysis and detailed link analysis in Table 5.

4.2.2 Architecture Baseline

The R2C2 team created the Architecture Baseline to act as a graphical representation of how different functionalities of the R2C2 interact. Each box on the Architecture Baseline represented an area that was filled by a physical component or software application during system design alternative generation. By filling every box with different design alternatives, a variety of designs were created, while still ensuring full system functionality in each scenario. The Architecture Baseline is better explained in Figure 12.

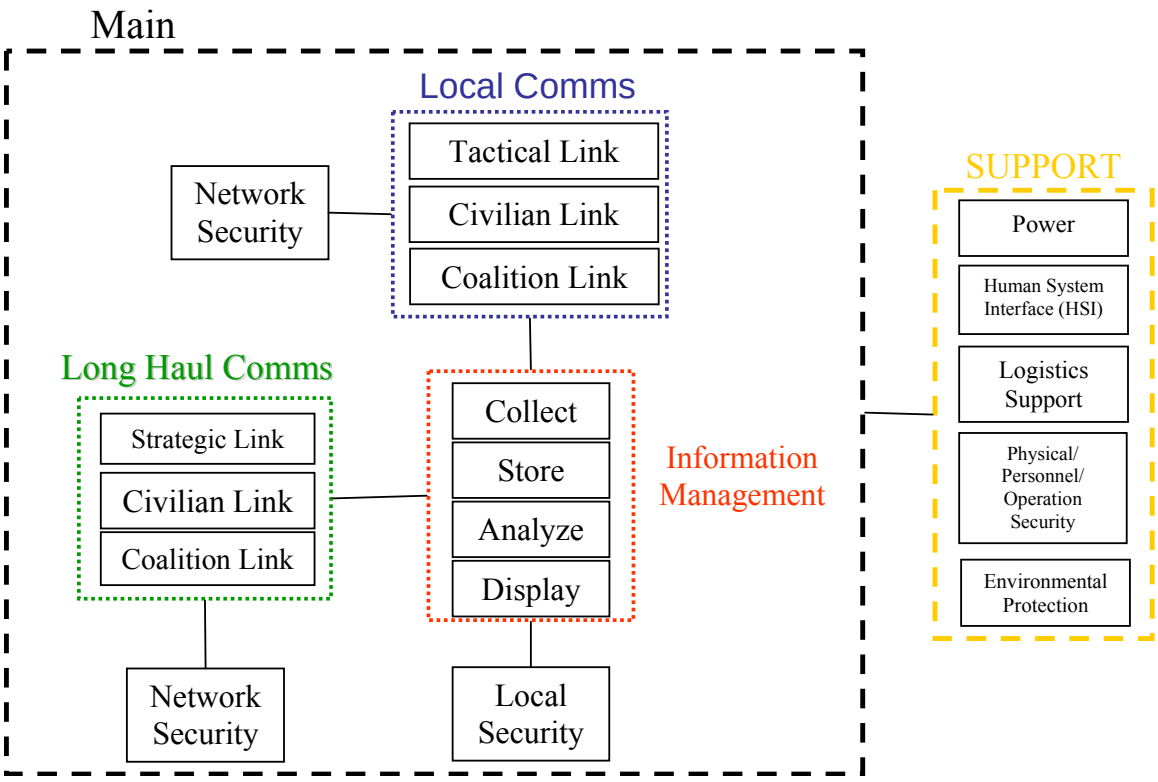


Figure 12: Architecture Baseline

The Architecture Baseline was broken into the Main toolset, outlined in a black dotted line, and the Support toolset, outlined in the yellow dotted line. The Support functions existed solely to ensure the Main aspects of the system were able function. Four Functional areas made up the Main aspect of the system: the Long Haul Communications (LHC) link, Local Communications (LOC) link, Information Management (IM), and security. The LHC area covered the strategic, civilian, and coalition communication links that were previously discussed. The LOC link offered communication capabilities to entities within the area of operation. This area covered the tactical link to supporting scouts and other local links to civilians and coalition partners. Next, the IM area included the collection, storage, analysis, and display of all data entering the system. The IM areas would ensure the most up-to-date SA software was integrated and accurate for local, organic, and command entities. The last subset of the Main toolset was security, outlined in solid black. Security fed into the LHC, LOC, and IM systems to reduce the risk of data corruption and to maintain its integrity.

The Support toolset consisted of five functional areas that were integral to Main system operation: Power, Human System Interface (HSI), Logistics Support, Physical/Personnel/Operations Security, and Environmental Protection. Power and HSI were the most important areas of concern. The Power subset addressed whether there was a need for a portable R2C2 power source. HSI, in this case, referred to the transportability and packaging of the system and forced system designs to incorporate lightweight and compact components.

4.2.3 Market Analysis

Given the broad spectrum covered by the Main and Support toolsets, many different methods and equipment were identified as possible solutions to areas of the Architecture Baseline. In order to fully identify all methods and equipment, a market survey was completed by the R2C2 team. The team was divided into smaller groups to research areas of communications, IM, and power. All researched equipment and software were geared towards creating a small, portable unit for use in an austere location. The findings of the survey are revealed in Sections 4.2.3.1.1 through 4.2.3.1.4.

4.2.3.1 Communication Alternatives

Communication systems are comprised of a sender, a receiver and a transmission medium over which the information travels. The objective is to ensure the meaning assigned to the data is recovered with minimum degradation. The mobile R2C2 communication system focused on transferring three critical types of information: voice, video, and data. The market survey was conducted to identify all means to transport information via a local and long haul link. From mission analysis, it was assumed that hard-line, terrestrial infrastructure was not reliable or available for communications and all links must be achieved through the free space environment.

4.2.3.1.1 Local Voice Communication. Local communication alternatives were broken down into voice and data options. Table 6 shows common, present-day voice communication devices. Information on the size, weight, number of components, infrastructure, security, and coverage were identified for each communication method. These were selected to facilitate the selection of voice

equipment that could easily be integrated into the R2C2 without a significant addition in weight or a reduction in capability.

Device	Size	Weight	Number of Components	Infrastructure Needed	Secure	Coverage
Satellite Phones						
Globalstar[58]	Handheld	Ounces	1	Space	No	Global
Iridium[59]	Handheld	Ounces	1	Space	Yes	Global
Radio Phones[60]	Handheld	Ounces	1	Terrestrial	No	Local/Extendable
Cell Phones	Handheld	Ounces	1	Terrestrial	No	Local
Personal Cell System[61]	Handheld	Ounces	Many	Personal	No	Extendable Local
Military Radio						
Manpack Radio[62]	15 x 10 x 4	20 pounds	1	None	Yes	Beyond LOS
LMR[63]	Handheld	Ounces	1	Space	Yes	LOS

Table 6: Voice Communication in the Local Environment

Satellite phones were selected because they are currently used worldwide by traveling businesses and during military operations. These phones are small and lightweight, but require a user to be within a satellite coverage zone. Satellite phone constellations travel in Low Earth Orbit (LEO) patterns and operate within the L Band. Globalstar and Iridium satellite phones are comparable in capability, but the U.S. military currently has a contract with Iridium Satellite LLC.

Radio phones were researched because they are a means of communication used in countries all over the world. In many Third World countries, Radio phones are used predominantly for police and government communication. Radio phones use a frequency within a country's radio spectrum and operate by utilizing the national radio tower communications infrastructure. Any individual with a Radio phone can set the correct frequency and transmit over a long range because the signal is relayed from tower to tower. Although the Radio phones can transmit long

[58] Globalstar, Inc. Company Website, http://www.globalstar.com, April 2006.

[59] Iridium Satellite Company Website, http://www.iridium.com, March 2006.

[60] Interview between Dr. Gary Langford, Professor, NPS and ENS James Colgary, Student, NPS, 1 March 2006.

[61] IP Access, "Nano BTS," http://www.ipaccess.com/products/nanoBTS.htm, March 2006.

[62] Interview between Capt Kevin Stoffell, USMC, Student, NPS and ENS James Colgary, Student, NPS, 29 March 2006.

[63] Ibid.

distances, all transmissions are subject to interception because encryption does not commercially exist.[64]

Cell phones are in common usage all over the world. Given that the cell infrastructure only exists in highly populated areas, the use of cell technology in far removed locations is not possible. The internationally recognized cell phone standard is GSM. Cell phones will only function if within a working coverage area, the individual has subscribed to a cell phone service provider, and the individual has a compatible cell phone. Currently, transmission over cell phones can be intercepted and easily interpreted. The encryption standard used by GSM has been deemed vulnerable by international cryptologists.[65]

A personal cell system is a relatively new concept that allows individuals to set up or expand a small cell phone infrastructure. This technology is useful in locations that do not receive acceptable cell phone coverage. Small transceiver devices are setup in a method to expand cell phone coverage over a particular area. The transceiver can link back to a commercial cell system or act as an independent system for multiple users to communicate only with one another.

Military radio uses Government-Off-The-Shelf (GOTS) products that are commonly used in the field for voice communications between soldiers. Both manpack radios and handheld Land Mobile Radios (LMRs) were chosen to represent this category. Manpack radios and LMRs can operate in the same frequency spectrum, but manpack radios provide an additional link power to send voice transmission further than standard LMRs.[66]

4.2.3.1.2 Local Data Communication. Table 7 displays the data communication options for local communications. The number of components needed, power requirements, security of transmission, data rate, and coverage area for available technology was collected.

---

[64] Interview between Dr. Gary Langford, Professor, NPS and ENS James Colgary, Student, NPS, 1 March 2006.

[65] Ibid.

[66] Interview between Capt Kevin Stoffell, USMC, Student, NPS and ENS James Colgary, Student, NPS, 29 March 2006.

	Power Required	Secure	Data Rate	Coverage
Wireless Personal Area Network (PAN)[67]	Low	No	2 Mbps	10 m
Wi-Fi: 802.11b[68]	Med	Yes	11 Mbps	30 m
Wi-Max: 802.16[69]	High	No	70 Mbps	50 km

Table 7: Data Communication in the Local Environment

The wireless PAN is a very short range means of data transfer. This technology is commonly used to facilitate "hands free" and local (within 10 m) data transfer of large files. Utilizing a wireless PAN can reduce wire clutter and overall equipment weight, but remains unsecured and only useful in short range.

802.11 (Wi-Fi) is the most common wireless protocol. It allows for a high data transfer rate over a wide area. One wireless router can support multiple users over a 30-meter radius. Wi-Fi eliminates the need for wires connecting each computer and greatly increases a user's mobility. Currently, only 802.11b is National security Agency (NSA) certified to be secure using a SECNET 11 device.[70] 802.11 "a" and "g" are not supported by an approved security standard.

802.16 (Wi-Max) wireless technology is a long range, high bandwidth protocol. Current employment of Wi-Max technology is in a point-to-point configuration and requires a large amount of power. Two Wi-Max antennas must point directly at one another to successfully transmit data. Data transmission ranges have exceeded 50 km in coverage.[71] Wi-Max technology can be coupled with Wi-Fi to transmit data over a long range and create a local access point for standard Wi-Fi users.

4.2.3.1.3 Satellite Constellations Used for Long Haul Communications. Table 8 displays the various satellite constellations that can be used for long haul communications. Constellations were organized into Geosynchronous Earth Orbit (GEO) and LEO groupings. GEO satellites orbit at an altitude of 22,000 miles,

---

[67] Mobile Computing Definitions, "PAN," http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html, May 2006.

[68] Wikipedia, "802.ll," http://en.wikipedia.org/wiki/802.11b, March 2006.

[69] BluePrint Wi-Fi Report I.

[70] Harris, "Secure Communications Solutions," http://www.govcomm.harris.com/secure-comm/, May 2006.

[71] Caroline Gabriel, "Wi-Max: The Critical Wireless Standard," BluePrint Wi-Fi Report I, 1 October 2003, p. 4.

while LEO satellites orbit at an altitude between 312 miles and 1,242 miles.[72] In order to successfully transmit over the long GEO range, a ground terminal must transmit at a higher power than small or handheld LEO satellite communication devices. The altitude of a satellite system has a direct impact on the time it takes to send a message from one location on the earth to another. The higher the orbiting altitude, the longer it takes for a message to reach the recipient.

Satellite	Primary Band	BW (Mbps)
GEO		
Commercial		
INMARSAT[73]	L	<0.125
Intelsat	Ku	Dependent on terminal
Eutelsat	Ku	Dependent on terminal
Hispasat	Ku	Dependent on terminal
Eurpoestar	Ku	Dependent on terminal
IPStar	Ku	Dependent on terminal
ShinSat	Ku	Dependent on terminal
AsiaSat	Ku	Dependent on terminal
Military		
DSCS[74]	X	Dependent on terminal
Milstar[75]	X	<1.544
MUOS[76]	UHF	<0.0625
LEO		
Globalstar[77]	L	<0.01
Iridium[78]	L	<0.01

Table 8: Satellite Constellations Available for Use

GEO satellites were organized into commercial and military categories. Commercial constellations require satellite transmission in Ku Band, while military systems require transmission in the X Band. The Commercial INMARSAT and the military's Mobile User Objective System (MUOS) operate in different bands.

---

[72] Tin Hua Lee, "An Analysis of Emerging Commercial Wide Band Satellite System and Their Potential for Military Use," http://handle.dtic.mil/100.2/ADA361515. Last accessed in May 2006.

[73] Inmarsat Company Website, http://government.inmarsat.com/solutions/default.aspx. Last accessed in April 2006.

[74] Chairman, Joint Chiefs of Staff, Joint Publication 6-0, *Joint Communications System*, 20 March 2006, pp. 11-10.

[75] Ibid., pp. 11-12.

[76] Bryan Scurry, "Mobile User Objective System (MUOS)," Presentation given at the Norfolk Convention Center, Norfolk, VA, 29 June 2005.

[77] Globalstar, Inc., Company Website, http://www.globalstar.com, April 2006.

[78] Iridium Satellite, Company Website, http://www.iridium.com, March 2006.

INMARSAT requires users to purchase an INMARSAT satellite dish and operate in the L Band. Other commercial constellations can accommodate any satellite dish as long as the terminal supports the required frequency. Additionally, INMARSAT only supports up to 0.125 Mbps, while other satellite constellations provide as much throughput as the designated ground satellite terminal can support. The military MUOS satellite system operates in the UHF frequency spectrum and supports only voice communication. This system has been put into place to globally connect ground forces without reliance on a commercial provider.

The Globalstar and Iridium satellite constellations can provide a data transfer capability to users worldwide, in addition to normal voice communication. The small terminal required for the LEO constellations makes data products appealing, but the data rates available on each system are less than 0.01 Mbps. The slow Globalstar and Iridium data rates would not adequately support users trying to access a SIPRNET or NIPRNET account.

4.2.3.1.4 Satellite Terminals Used for Long Haul Communications. The last aspect researched for the communications market survey was portable ground terminals. Only Very Small Aperture Terminal (VSAT) satellite systems that had the ability to access commercial and military satellite constellations and were capable of sending information over Internet Protocol (IP) were investigated. Furthermore, VSAT systems had to have a dish size of less than one meter, a throughput of 2.0 Mbps or greater, and a total weight of less than 100 pounds. These specifications were set in order to limit research to satellites that were man-transportable, while still meeting both CPD and BAA technical requirements. Five VSAT terminals were identified that met the size, throughput, and weight standard. Information on all remaining VSATs was collected concerning their operating bands, system weight, transmit/receive rate, setup time, power consumption, stowed dimension, military standards compliance, licenses, and iDirect capability. iDirect was important during satellite selection because it provides the most reliable IP modem for transmission via satellite.[79] Additionally, iDirect is the only

[79] iDirect, "iDirect Technologies Broadband VSAT System – Summary," www.idrect.net, May 2006.

IP solution authorized for military Advanced Encryption Standard (AES).[80] Table 9 shows an abbreviated compilation of VSAT specifications. Appendix D contains a more detailed table showing specifications for each of the previously stated categories.

Sat System	Bands			Weight		Transmit Rate	Receive Rate	Setup Time	Power Consumption
	X	*Ku*	*Ka*	*lbs*	*# of Cases*	*Mbps*	*Mbps*	*min*	*W AC*
Norsat Globetrekker[81]	Optional	Yes	Optional	<50	1	4	4	<10	480
Norsat U.P. 5200[82]	Optional	Yes	Optional	46/46	2	8.448	8.448	10	480
SWE-DISH IPT-i Mil Suitcase[83]	Yes	Yes	Optional	86	1	4	4	5	650
TCS DVM-90[84]	No	Yes	No	40	1	2.4	2.4	20	500
GSI GlobeComm Auto-Explorer (.77m)[85]	No	Yes	No	48/50	2	4.2	4.2	15	375

Table 9: VSAT Terminals

4.2.3.2 Information Management (IM) Applications

IM applications help users to manage the information gathered from various sources, whether they are organic or inorganic. An effective package of IM tools handles the collection, analyzing, displaying, and storing to give the user optimal SA. Commercial, as well as military software suites, currently exist that fulfill the need for IM. Identified from the market survey were three key attributes that must be encompassed within a complete IM package: geospatial information application, a collaborative information environment (CIE) application, and digital storage.

Geospatial information applications provide a variety of maps, satellite images, elevation contours, and interactive drawing tools for mission planning and operations. Google Earth®, ArcView®, and Microsoft Terraserver® are commercial software products with which the user can see multiple images of a location from

---

[80] Telephone conversation between Mr. Joseph Harry, STEP Site Operations Technician, Camp Roberts, CA, and LCDR Lisa Sullivan, Student, NPS, 15 May 2006.

[81] Norsat, *Norsat Globetrekker Brochure*, http://www.norsat.com/pdf/download/UPT.pdf. Last accessed in April 2006.

[82] Norsat, *UP 5200 Brochure*, http://www.norsat.com/pdf/download/Norsat%205200Ku-10W-P3K.pdf. Last accessed in April 2006.

[83] SWE-DISH, *SWE-DISH IPT-I Mil Suitcase Brochure*, http://www.swe-dish.se/upload/_PDF/SWE-DISH%20IPT%20MIL%20Suitcase%202006.pdf. Last accessed in April 2006.

[84] TeleCommuncations Systems, *TCS DVM90 Brochure*, http://www.telecomsys.com/downloads/government/pdf/brochure_DVM90.pdf. Last accessed in April 2006.

[85] GSI GlobeComm, *Auto-Explorer Brochure*, http://www.globecommsystems.com/pdf/0.77%20Auto%20explorer.pdf. Last accessed in April 2006.

different angles and virtually fly in and around the location of interest. These SA functions are useful for mission planning, rehearsal, and execution. While commercial products are user friendly and open source, they do not include the most updated satellite imagery. There are many military products that provide the same functions with high resolution Digital Terrain Elevation Data (DTED). FalconView is one example of a GOTS system that was originally used for flight planning, but is now being used by ground forces.[86] In addition to mapping software for mission planning, a COP capability that displays an updated battle space environment of terrain, weather, enemy forces, and friendly forces will be provided by the military product Global Command and Control System-Joint (GCCS-J).

A CIE utilizes software tools to allow a virtual meeting and workspace between different users that are geographically separated. DJC2 systems, including the RRK, will include the Defense Collaboration Tool Suite (DCTS) and Information Workstation (IWS) to meet the requirement to allow a CIE "to facilitate parallel operations among RCCs, joint force headquarters, the service components, and other organizations that are separated by time, organizational boundaries, and geography."[87] Groove Virtual Office® is a commercial collaborative tool suite that offers peer-to-peer access anywhere through the Internet, virtual meetings, file sharing, automatic encryption, alert notification, and instant communications via chat or voice. Groove has been successfully used by NPS HFN, TNT, COASTS groups and national agencies, such as Homeland Security, for disaster relief exercises and operations and has been approved for use in the DCTS.[88]

Digital storage refers to computer components, devices, and recording media that retain binary information for an interval of time. Digital storage played an important role in the R2C2 environment. The most applicable type of storage to the system was nonvolatile storage. Non-volatile memory is not affected by inconsistent power supply and can retain data for an indefinite period. It allows important data and

---

[86] Chris Bailey, Senior Research Engineer, "Reference Department of Defense Usage of FalconView™," http://www.falconview.org/events.htm. Last accessed in March 2006.

[87] DJC2, CPD, OPNAV N71C2-668(1)-71-05, 30 November 2005, p. C-10.

[88] Groove Networks Website, www.groove.net. Last accessed in March 2006.

information captured by the scouts, such as images and video, to be stored in the devices. It also provides storage for all the information processed by the R2C2 applications.

Currently, there are three types of nonvolatile storage which are applicable to the R2C2 environment: magnetic, optical, and flash memory storage. Magnetic storage uses different patterns of magnetization on a magnetically coated surface to store information. The floppy disk and the hard disk are examples of magnetic storage. These two types of storage could be found in the R2C2 laptops, although floppy disk drives are fast becoming obsolete items. The storage capacity of the hard disk in the COTS laptop ranged between 40 Gigabytes (GB) and 100 GB. Optical disc storage uses tiny pits etched on the surface of a circular disc to store information, and reads this information by illuminating the surface with a laser diode and observing the reflection. Some of these include CD, DVD, CD-R, DVD-R, etc. The last type of storage applicable to R2C2 was flash memory. Flash memory is a form of rewritable memory chip that is small and easily transportable to any system with a common interface. Flash memory on the market included a variety of sized Secure Digital (SD) cards, USB thumb drives, compact flash cards, multimedia cards (MMC), memory sticks, and smart media. The benefit of using such devices is the ultra-portability, but it is limited to a current maximum of 4 GB of storage.[89]

4.2.3.3 Power Alternatives

Power alternatives researched in the market survey aimed to fulfill a small, portable, long-lasting option that could sustain a communication system. Categories of power researched were: gas generators, batteries, fuel cells, solar, and wind power systems. The best-performing product in each category is identified in Table 10. Generators proved to output the most power, while solar and wind devices were capable of the second largest power output. Solar panels, however, required significant sunlight and the wind turbine required a very fast wind speed. External batteries researched did not output a comparable power rating as the previous alternatives, but were very small and retained the ability to be placed in series to provide a large amount of power. Micro

[89] Wikipedia, "Computer Storage," http://en.wikipedia.org/wiki/Digital_Storage. Last accessed in May 2006.

fuel cells were found to produce a comparable amount of power to batteries, last significantly longer, and are in a smaller package. Unfortunately, micro fuel cells have not yet achieved commercial maturity.

Power System	Wattage Output	Size (inches)	Weight (lbs)	Max Run Time (hours)	Environmental Concerns
Honda Generator (portable)[90]	2,000	20.1 x 11.4 x 16.7	46.3	15	Need gas
External Battery					
BA5590 Military[91]	90	6 x 4 x 2	2.2	2.3	None
N-Charge[92]	90	9.05 x 11.8 x 0.5	2.96	1.4	None
Micro Fuel Cell[93]	90	2.6 x 2.6 x 2.6	1.06	7.2	None
Solar[94]	1,350	12.3 x 15.6 x 38	94.6	19	Need light
Wind[95]	1,000	51 x 20 x 13	65	Wind dependent	Need 26 mph wind

Table 10: Power Systems

4.3 GENERATION OF R2C2 SYSTEM DESIGN ALTERNATIVES

As seen from the market survey results, many solutions existed to create a small, rapid response, communications unit. The R2C2 Architecture group selected the best alternatives for each functional area highlighted in the Architecture Baseline. All tradeoffs were done under the assumption that local infrastructure was unreliable and/or nonexistent and the overall system design had to be small. These assumptions were taken from the mission and requirements analysis done in previous chapters.

4.3.1 Local Communications (LOC) Link

The number of local link alternatives generated by the market survey was reduced as a result of the DJC2 JPO's suggestion that the R2C2 team focus only on LOC voice

---

[90] Honda, "Super Quiet Inverter Generators," http://www.hondapowerequipment.com/gensup.asp. Last accessed in May 2006.

[91] David Morrison, "Micro Fuel Cell Demonstrates High Power Output," http://powerelectronics.com/news/fuel-cell-output/. Last accessed in May 2006.

[92] Valence Technology, Inc., "Why Compromise Military Safety with Traditional Lithium-ion Batteries?" http://www.valence.com/pdffiles/Military_Datasheet.pdf. Last accessed in May 2006.

[93] Morrison, May 2006.

[94] SolarSense, "Nomad 1500 Pro Series," http://www.solarsense.com/Products/1-Complete_Systems/3-NOMAD_1500/NOMAD_1500.html. Last accessed in May 2006.

[95] Southwest Windpower, "Whisper 100/200 Specification Sheet," http://www.alpinesurvival.com/Whisper_100_200_Spec_Sheet.pdf. Last accessed in May 2006.

connectivity. The number of voice alternatives was reduced from the seven identified in the market survey down to three. This was done by eliminating those means that were reliant on terrestrial infrastructure and incapable of secure voice transmission. Military manpack radios, LMRs, and Iridium satellite phones were therefore selected as R2C2 local voice alternatives. These methods were explored further in Chapters 5.0 and 6.0 to determine which LOC method was optimal for R2C2 use.

Although the DJC2 JPO recommended the LOC link consist solely of voice alternatives, the R2C2 team decided to establish an LOC alternative that would allow for high bandwidth data transfer over a long distance. The data link encompassed two technologies identified in the market survey: 802.16 (Wi-Max) and 802.11 (Wi-Fi). This decision was made to determine whether or not a data link would truly add value to the LOC link used by the scouts operating in the field. Because a significant amount of research with the Wi-Max and Wi-Fi protocols has been done by the COASTS, TNT, and HFN groups at NPS, the addition of a similar link into the R2C2 system was chosen in order to explore its effectiveness in a small C2 unit. Link models were created to evaluate the LOC data link and were analyzed in Chapters 5.0 and 6.0.

4.3.2 Long Haul Communications (LHC) Link

Long haul communication via a satellite relay was determined to be the only viable means of IP communication. Long haul reachback alternatives, using sky waves, ground waves, or terrestrial relay systems, were ruled out due to significant range and bandwidth restrictions. Therefore, the utilization of a GEO satellite connection was determined to be the only option for high bandwidth voice, video, and data transfer between the R2C2 and the RCC.

Satellite information transfer for a military application can transit by way of the "front door" method, "back door" method, or VPN Gateway. Trade-offs for these three methods concerned the security level/layers required as well as the amount of network equipment needed by the user.

The front door method of data transfer is an extremely secure means of communication. Data can be sent from a ground terminal via any location on earth that is within the coverage area of a commercial or military satellite. Before the data is sent

from a ground terminal to a satellite, it must pass through an OSI Layer 1 security measure: bulk encryption. Bulk encryption is a method by which the security of an entire piece of data, including its intended destination, is concealed. Bulk encryption can be achieved through the use of a separate bulk encryption device or AES. AES software, however, is permitted only when using an iDirect IP modem.[96] Once the data package is encrypted, it is relayed off a satellite and sent to a military owned and operated ground station called a Teleport. Standardized Tactical Entry Point (STEP) sites, Naval Computer and Telecommunications Area Master Stations (NCTAMS), and other Defense Information Infrastructure (DII) gateways were combined under one name, a Teleport, which handles military correspondence from all over the world and directs it to its destination within the GIG. After the Teleport has accepted the data transmission and decrypted the destination, the Teleport routes the request to NIPRNET, SIPRNET, or another destination.

The back door method allows a global user to send information right to the RCC, bypassing the Teleport ground station. This method of data transfer allows the RCC to set his own encryption standards. The global user then accesses the GIG through the RCC's network router.

The last method that can be used to transmit data via a satellite is creating a Virtual Private Network (VPN) Gateway to the RCC. The VPN can be created through the public Internet, allowing R2C2 operators to create a direct tunnel to the RCC's base network. VPN tunneling to the RCC virtually puts an operator at the command headquarters, giving them full access to NIPRNET, SIPRNET, and GIG information. Utilizing a VPN falls under Layer 3 security. This method does not require any bulk encryption, just access and subscription to a satellite constellation that is also an Internet Service Provider (ISP). Currently, the 86th Air Force Space and Communications Squadron uses the VPN solution for reachback when operating their own small communications unit.[97]

---

[96] Telephone conversation between Mr. Joseph Harry, STEP Site Operations Technician, Camp Roberts, California, and LCDR Lisa Sullivan, Student, NPS, 15 May 2006.

[97] Interview between Capt Johnny Hill, USAF, 86th Space and Communications Squadron, Kaiserslautern, Germany, and authors, 12 April 2006.

In order to reduce the amount of equipment while still maintaining the highest amount of possible security, the Architecture group determined that utilizing an AES encryption to access a Teleport ground station was the most appropriate method for the R2C2 system. Subsequently, this required the selection of a VSAT terminal that supported iDirect technology.

Due to the selection of an AES and the need to connect to a GEO satellite, the ground terminal had to be significantly evaluated to ensure the most appropriate one was selected. Without an effective, capable, and reliable terminal with global reachback, the R2C2 system can not fulfill its intended mission. From the VSAT terminals identified in the market survey, each was evaluated to choose the terminal best suited for the R2C2. Weight, size, iDirect capability, and current licensing were pronominally compared. Further detail on VSAT evaluation is found in Chapter 6.0.

4.3.3 Information Management (IM)

Alternatives generated for the R2C2 IM portion of the Architecture Baseline consisted of a network architecture as well as different software packages to aid in SA.

4.3.3.1 Network Design

To create a network that accomplished SIPRNET, NIPRNET, and CENTRIXS reachback capability, many outside system matter experts were consulted to help in design of the system. As a result, the network design was done at a high level and touched on integral parts of the network design like SIPR, NIPR, and CENTRIXS encryption requirements. Figure 13 is a graphical representation of the network constructed for R2C2.

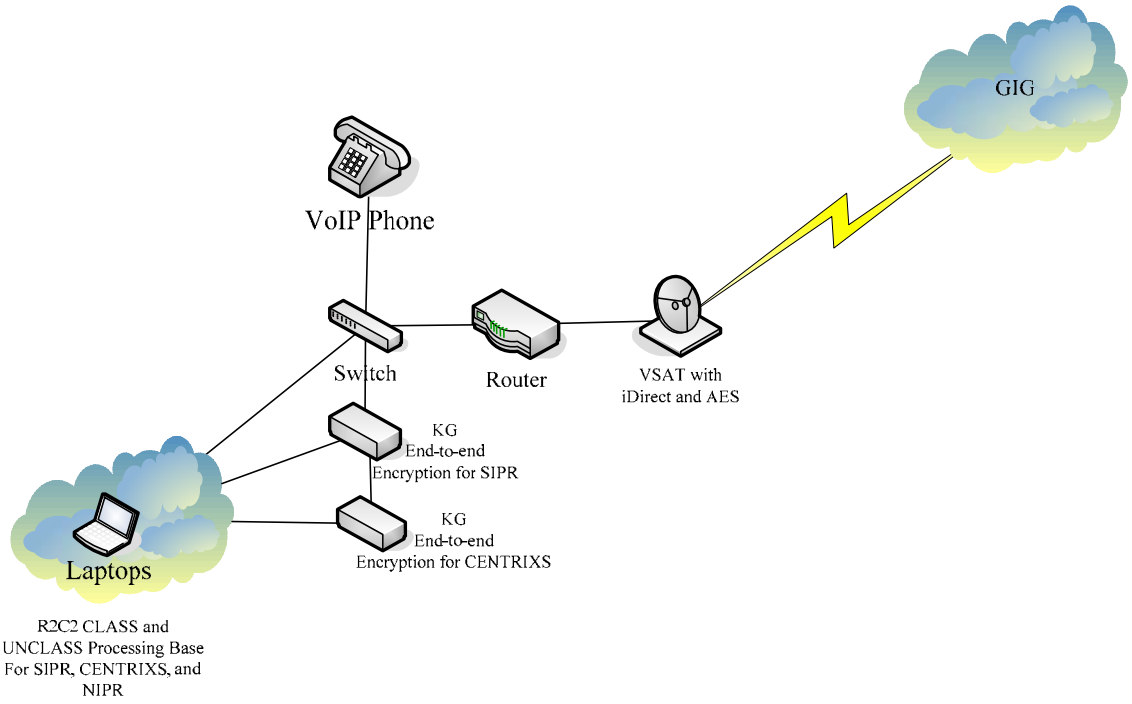


Figure 13: IM Network Design

Included in the network design are laptops (single with interchangeable hard drives or multiple single hard drive units), encryption boxes, VoIP phone, switch, router and a portable VSAT. Laptops were selected over personal computer (PC) towers because they possessed equal computing capability, while being significantly more mobile. The VoIP was included to meet requirements for a voice connection over an IP long haul connection.

The most important aspect of the above diagram was how a NIPRNET, SIPRNET, and/or CENTRIXS connection was established through the use of a satellite. As was previously discussed, the network configuration was streamlined and simplified by the selection of a VSAT with iDirect technology to allow for AES software bulk encryption. The network configuration requires that all data sent via the VSAT is bulk encrypted. Since NIPRNET requires no end-to-end encryption, it is only bulk encrypted before being sent over a satellite link. Once the computer establishes a connection to the GIG, all data is routed directly to the NIPRNET. In order to access SIPRNET, the data traffic must be end-to-end encrypted by an encryption device. There is currently no software application that can be substituted for the physical encryption component. The data can then pass through an ordinary switch and router combination before being sent

out over a standard Ku or X band transmission. The coalition network, CENTRIXS, can only be accessed through SIPRNET and has encryption standards on top of those needed for a standard SIPRNET connection. Therefore, data being passed via CENTRIXS is end-to-end encrypted twice and bulk encrypted once before leaving the satellite terminal.[98]

In the current configuration, one laptop can access NIPRNET, SIPRNET, and CENTRIXS. The hard drive, however, must be changed out before transitioning to each network.[99] Alternately, three separate computers could access each network simultaneously as long as satellite bandwidth allows it.

In the event that an extended LOC data link was integrated into the network, there would be a distinct separation of the two networks with the use of an additional server and firewall. The graphical representation in Figure 14 shows the network integration.

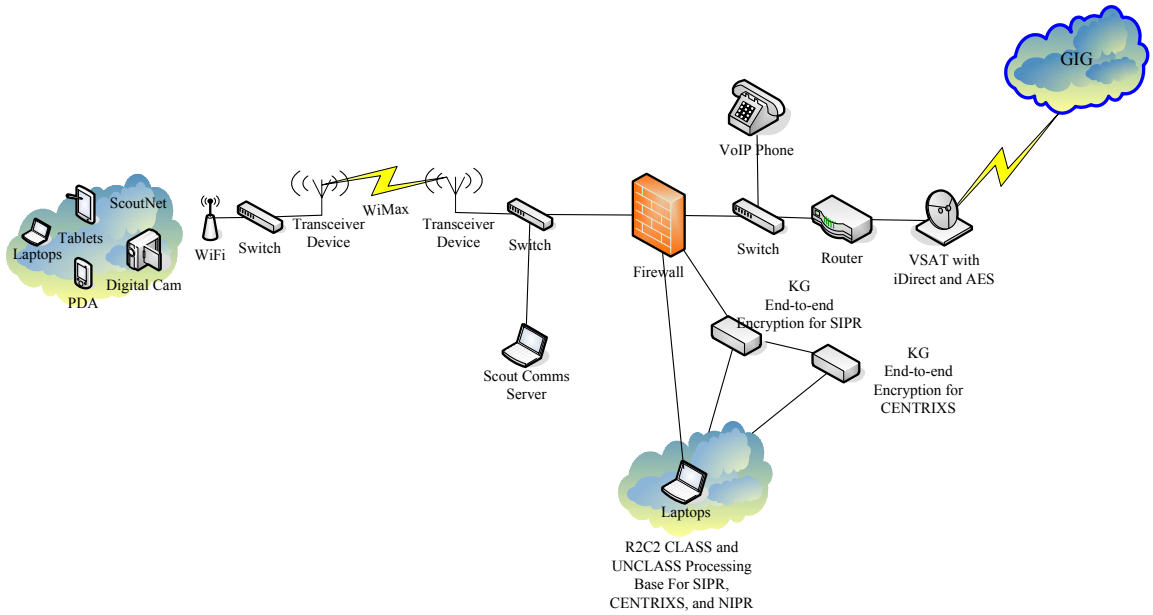


Figure 14: Integrated LOC Network

By placing the R2C2 laptops behind an external server and firewall, the R2C2 operators have control over the data that comes into the system from the scouts and the RCC. Given that the scout's sole mission is to pass information, they do not need

[98] Teleconference between Mr. Steve Grant, R2C2 Systems Engineer, and the R2C2 team, 31 January 2006.

[99] Interview between the DJC2 JPO and the R2C2 team, 29 March 2006.

direct access to the Internet—a location to offload important data is sufficient. The Scout Server gives the scouts access to offload data as well as confirmation it was sent and received. Because of the potential vulnerability of the LOC link, the firewall and the external server help protect the R2C2 laptops from being compromised. Additionally, they stop the scouts from using long haul bandwidth. When the R2C2 operators need information from the scouts, they retrieve it from the Scout Server. If real time video back to the RCC is required, a change can be made to the firewall in order to allow a direct feed from the scouts to the RCC. Lastly, the server allows a place for the R2C2 to host a collaborative network to ensure scouts can view an updated COP.

4.3.3.2 Software Package

The selection of a proper software package for IM was selected based on the system needs. The market survey revealed many different geospatial applications and CIEs that are necessary to give a user better SA. DJC2 software build version 1.0.03 contains both types of SA applications the R2C2 team identified. By selecting the DJC2 software package, the R2C2 system achieved software commonality, interoperability, and a reduction in training requirements across DJC2 systems.

4.3.4 Security

This section will be expanded upon in the Security Appendix. Network, local, physical, personnel, and operations security concerns will be addressed.

4.3.5 Support

Alternatives generated from the Support portion of the Architecture Baseline were limited to concerns with power and HSI.

4.3.5.1 Power

From the market survey, many portable power options were identified. As per the identified requirements, just over 1,300 watts of power would be used by a functioning R2C2 Primary Suite. Power would have to be supplied organically by the R2C2 for a minimum of 10.5 hours and a maximum of 8 weeks. Given the varying duration the R2C2 would have to supply its own power, the R2C2 team determined that

designing a stand alone C2 system without organic power would be an incomplete design.

From the market survey, multiple power sources were identified. The alternatives were pared down from six to two alternatives. Small generators and batteries were concluded to be the only reasonable means to provide sufficient power to the entire R2C2 system. Solar and wind energy sources proved to be too large for a two-person portable team and did not offer enough power if scaled down in size. Lastly, micro fuel cell technology may a viable option for future development, but is currently too immature and incapable of providing over 1,300W for a sustained period. A battery-powered R2C2 system would last a maximum of roughly 1.5 hours operating on 10 batteries. This was an average time based on the wattage consumed by each component in the system. For any period of time longer than 1.5 hours, new batteries would have to be used because expended batteries could not be recharged. A small generator, however, could support up to a 2,000W system for over 15 hours on a single tank of fuel (1.1 gallons). However, fuel must be located and purchased after arriving in the area of operation. Chapter 6.0 provides deeper analysis into the selection of an organic power source.

4.3.5.2 Portability (HSI)

Alternatives for portability were addressed throughout the alternative generation process. The Architecture group selected COTS equipment that can be easily packed away for each functional area of the Architecture Baseline. Commercial airline and military weight and size standards for carried luggage were taken into account to ensure the R2C2 system would meet transportability requirements. Most major airlines require carry-on baggage to be no larger than 45 linear inches (bag length, plus height, plus depth) and weigh no more than 40 pounds.[100] Normally, checked luggage can be no larger than 62 linear inches and weigh no more than 50 pounds. However, if checked luggage exceeds the free 50-pound weight allowance, a passenger must pay a fee to check luggage up to 100 pounds.[101] Military standards require that items carried over a

[100] Free Travel Tips, "Luggage Information," http://www.freetraveltips.com/Airlines/air03.htm. Last accessed in May 2006.

[101] Luggage Pros, "Luggage Restrictions," http://www.luggagepros.com/policies/luggage-restrictions.shtml. Last accessed in May 2006.

distance be no more than 45% of an individual's body weight. Additionally, items lifted three feet from the floor can weigh no greater than 87 pounds for males and 44 pounds for females.[102] The R2C2 system design incorporated rack mounts, foldable satellite dishes, and easily stowable network gear to ensure that integral equipment met commercial and military size and weight standards.

4.4 SUITE GENERATION

Throughout the alternative generation process and scenario elaboration, the R2C2 team acknowledged that the overall system design must be divided into specific suites of communications gear to facilitate better flexibility and scalability in operations. Figure 15 shows how the suites concept was integrated into the Architecture Baseline.

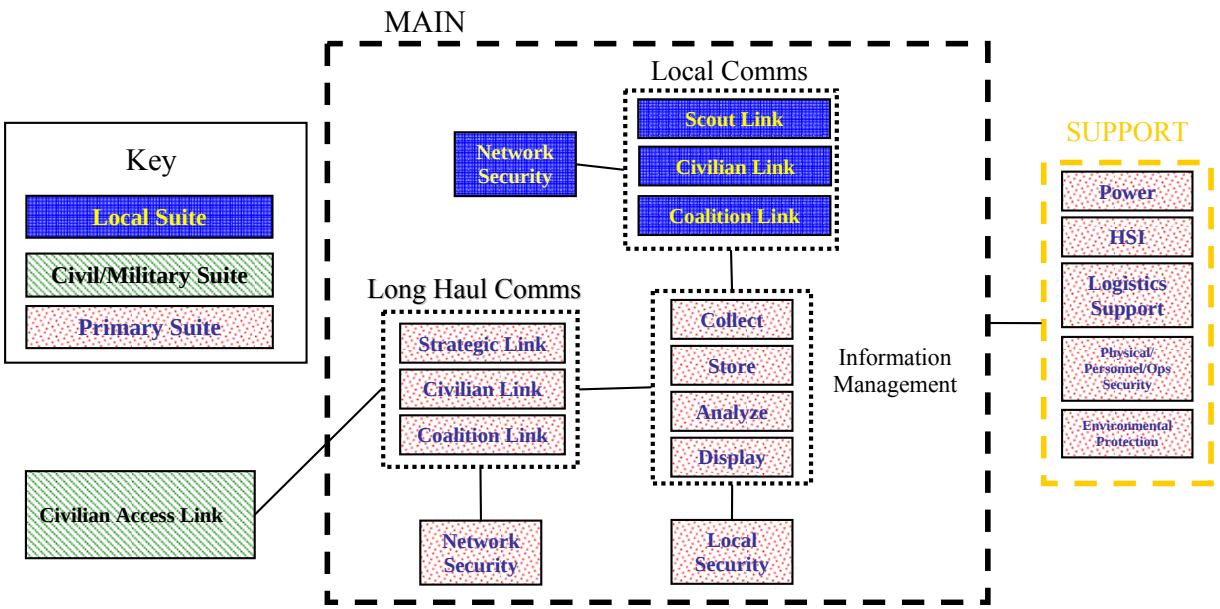


Figure 15: The Architecture Baseline with Suites Highlighted in Dotted Red, Solid Blue, and Lined Green

[102] United States Department of Defense, *Department of Defense Design Criteria Standard, Human Engineering*, MIL-STD-1472F (DoD), 23 August 1999, p. 139.

The Primary Suite (PS), highlighted in red, contains all IM components, LHC gear, laptops, VoIP phone, as well as all the support gear necessary for the given mission. The PS most closely represents the RRK system that was outlined in both the CPD and BAA. The Local Suite (LS), highlighted in blue, contains all communications gear that was needed for collaboration within the area of operation. This included gear to be stationed at the R2C2 PS as well as with the scouts. The integration of the CMS, highlighted in green, was placed outside the system because in the original Architecture Baseline, a node at which civilians could utilize the long haul connection did not exist. In the high-level picture, the CMS would integrate through the R2C2's long haul connection.

4.4.1 Primary Suite (PS)

The PS included the network configuration found in Section 4.3.3.1, Figure 13. The PS was the core part of the R2C2 system and can be used to establish R2C2 reachback capability for every mission.

4.4.2 Local Suite (LS)

The LS was a modular suite that can be added to the PS to fulfill local communication requirements in a given scenario. For instance, if it were decided that local communications were not necessary in the Counterterrorism Scenario because of the close proximity of the PS with the Special Forces, the LS could be left behind.

The LS contains three alternatives for further evaluation. The alternatives come from those generated and outlined in LOC link alternative generation, Section 4.2.1. The voice alternatives of military radios and satellite phones were further evaluated to determine which was best given the scenarios. Because military manpack radios and LMRs work on the same physical concepts, they were lumped into one alternative called military radio. The determination of the better system was evaluated on transmission reliability and coverage within a region in Chapters 5.0 and 6.0. The third alternative for the LS was a scout exclusive data network. The selected voice communications alternative would be coupled with a Wi-Max/Wi-Fi network to give system improvement

and redundancy. Decrease in data transfer time versus the amount of extra components the link required was evaluated in Chapter 5.0.

4.4.3 Civil/Military Suite (CMS)

The CMS was also a modular suite that could accompany the Primary R2C2 Suite on a mission when its functionality was needed. Specifically, the CMS would be useful in humanitarian assistance and disaster relief scenarios. Upon speaking with users familiar with HA/DR operations, the R2C2 team found that providing civilian counterparts access to the Internet as an incentive to share information and collaborate was an important concept. The reason for providing Internet access and interacting with civilian entities was previously expounded on in Chapter 2.0.

The CMS can be teamed with the PS in two ways: it can be integrated into the PS or exist as a separate entity with its own satellite dish. Figures 16 and 17 show both alternatives. The integrated CMS alternative functions by plugging directly into the existing PS router. Civilians would then use the PS satellite dish and share bandwidth with the R2C2 operators to access the Internet through the GIG. Bandwidth usage issues, as well as security issues, needed to be considered when integrating the CMS. These concerns were further investigated in Chapters 5.0 and 6.0. The second CMS alternative, bringing a separate CMS, increases the capability to civil organizations and decreases the burden on the PS system. Currently, the NPS COASTS and HFN programs have been doing research on a FLy-Away-Kit (FLAK) that sets up a mesh network of hot spots for civilians to connect to and gain Internet access. Further information on the FLAK can be found in Capt Lancaster's Thesis, "Developing a FLy-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)."[103] Bringing along a separate system involves a significant amount of extra equipment and personnel for setup and operation. Figures 16 and 17 graphically show the interaction of the integrated and separate CMS.

[103] David D. Lancaster, "Developing a FLy-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)," Master's Thesis, Naval Postgraduate School, Monterey, CA, June 2005.

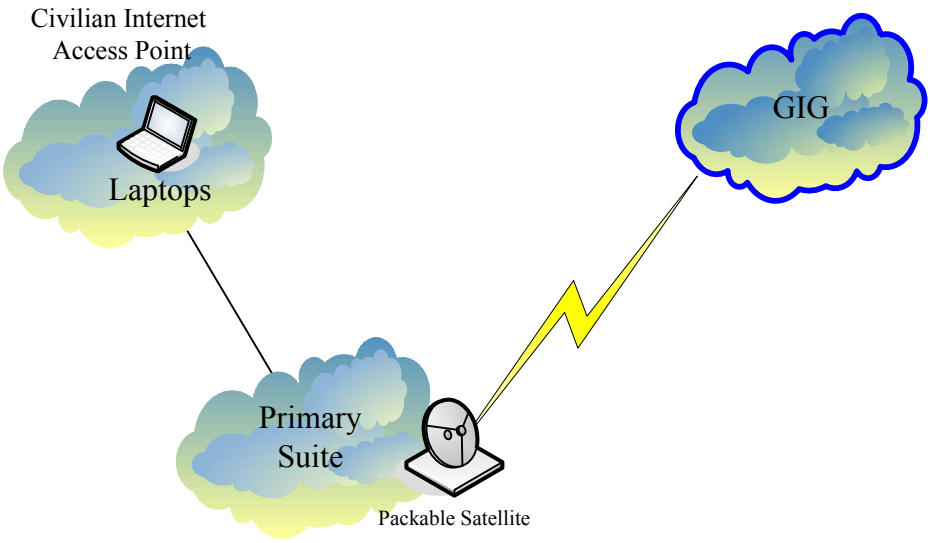


Figure 16: Integrated CMS

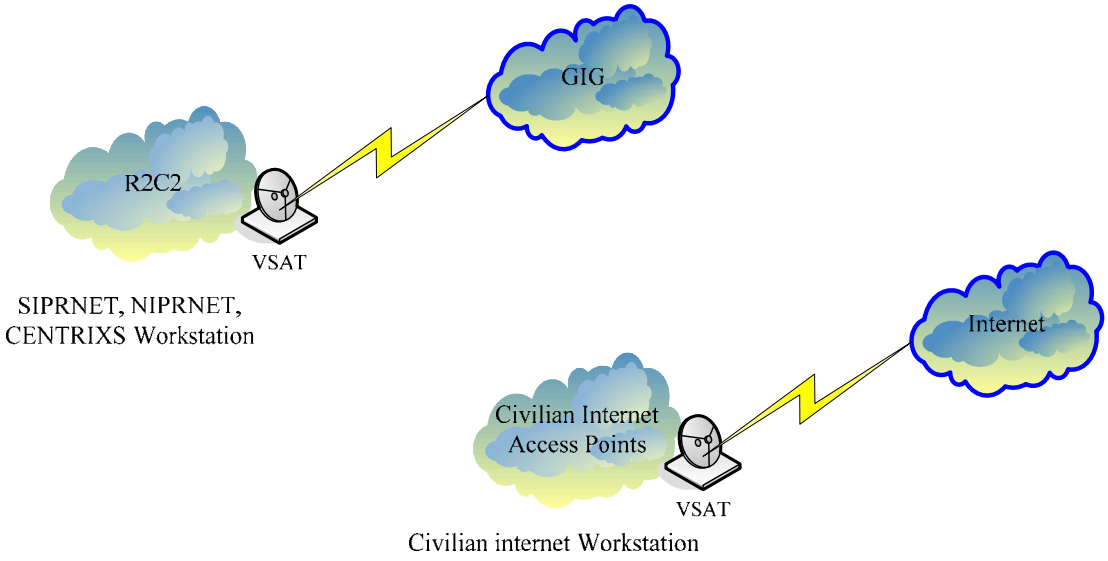


Figure 17: Separate CMS

4.5 CONCLUSION

System architecture design was done with enough detail to facilitate system modeling and analysis. Specific commercial Very Small Aperture Terminal (VSAT) satellite systems were identified because of their significant effect on overall system weight and performance. Alternatively, specific network gear or military radios were not

addressed in the detail of the satellite systems because it is assumed those components would be selected based on reliability and commonality of usage.

In summary, the system design facilitates a secure long haul reachback capability to SIPR, NIPR, and CENTRIXS networks via a VSAT. The central suite of the R2C2 was called the PS and contains all components needed to achieve successful reachback communications. Both an LS and a CMS are modular and can be added to the R2C2 mission package to further enhance the system's capability within the area of operation. The LS contains either military radios, satellite phones, or a Wi-Max/Wi-Fi data network. The CMS contains all the equipment necessary to provide Internet access for civilian HA/DR personnel, whether it is integrated into the PS or a separate system. The alternatives generated for each suite were modeled and analyzed in Chapters 5.0 and 6.0.

5.0 INFORMATION ASSURANCE

5.1 INTRODUCTION

Information Assurance (IA) plays a critical role in ensuring the confidentiality, integrity, and availability of information in the R2C2 system. The Information Assurance Technical Framework (IATF)[104] was used as the main guiding document in designing the R2C2 security architecture. The following sections of the chapter describe the Information System Security Engineering (ISSE) process used, the strategy adopted to protect the various enclaves, as well as the specific security components in the architecture. Some areas of research on Multi-Level Security (MLS), which may be useful of the future development of R2C2 system are included at the end of the chapter.

The design of the security architecture follows that of the R2C2 architecture baseline. The enclaves are defined by the Primary Suite, Local Suite and the Civil/Military Suite. Correspondingly, the boundaries exist between the different enclaves, between the Primary and Local Suites, between the Primary Suite and RCC, and between the Primary and Civil/Military Suites.

5.2 THE INFORMATION SYSTEMS SECURITY ENGINEERING PROCESS (ISSE)

The R2C2 team adapted the ISSE process from that expounded on in Chapter 3 of IATF document release 3.1. The process is developed based on three key principles, as listed in the IATF document:

a. Always keep the problem and the solution spaces separate.

b. The problem space is defined by the customer's mission or business needs.

c. The system engineer and information systems security engineer define the solution space, driven by the problem space.[105]

---

[104] United States Department of Defense, Directive 8500.1, "Information Assurance," 24 October 2002 and Instruction 8500.2, "Information Assurance (IA) Implementation," 6 February 2003.

[105] National Security Agency, "Information Assurance Technical Framework (IATF)," Release 3.1, September 2002, Chapter 3, p. 4.

The document also emphasized that the customer owned the problem. The system designed was to support the customer's mission or business. Though the customer owned the problem, it was suggested that the customer might not always be an expert in discovering and documenting the problem. The systems engineer and/or information systems security engineer should facilitate the customer in the formulation and documentation of the problem. Conversely, the systems engineer and the information systems security engineer were expected to be proficient in developing solutions. The challenge of the systems engineer and the information systems security engineer would be, however, to resist the customer's tendency to intervene/preempt in the design of the system as customer design inputs could become constraints on the final design and limit the SE design flexibility.

5.3 PROCESS

Based on the above principles, the ISSE process was conceived and the relevant phases of ISSE process had been adapted for the purpose of this project (as in Figure 18). The ISSE process supported the R2C2 SE Approach. The ensuing paragraphs elaborated on various ISSE phases and their respective linkages to each SE phase.

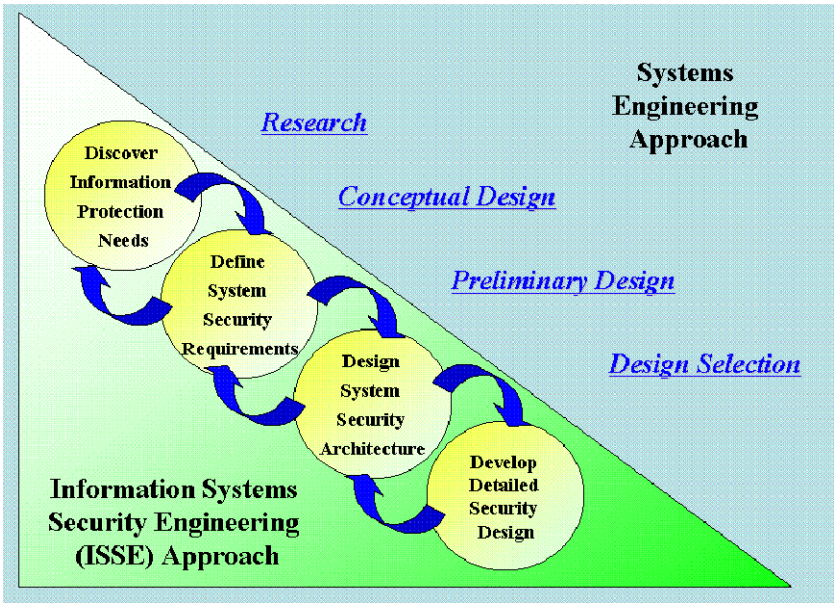


Figure 18: Relationship between Phases of SE and ISSE

Table 11 shows a comparison between the various phases of the SE and ISSE processes.

SE Phases	ISSE Phases
Research The systems engineer determined the customers. They assisted the customers to understand and document the information management needs that support the business or mission.	**Discover Information Protection Needs** The information systems security engineer facilitated the understanding of the information protection needs to support the mission or business with the customer. (the engineer didn't facilitate the customer) Statements about information protection should be documented.
Conceptual Design The systems engineer allocated identified needs to systems. Various scenarios were developed to scope the system environment and to link the allocation of system functions to that environment. A preliminary system CONOPS was written to describe operational requirements of the candidate system (or systems).	**Define System Security Requirements** The information systems security engineer allocated information protection needs to systems. A system security context, a preliminary system security CONOPS, and security requirements were developed.
Preliminary Design The systems engineer performed functional analysis and allocation by analyzing candidate architectures, allocating system requirements, and selecting mechanisms. The systems engineer developed the system architecture by allocating functions to selected components or elements and describing the relationships between the elements.	**Design System Security Architecture** The information systems security engineer worked with the systems engineer in the areas of functional analysis and allocation by analyzing candidate architectures, allocating security services, and selecting security mechanisms. The information systems security engineer developed the security architecture by allocating security functions to selected components and elements and describing the inter-components interactions.
Design Selection The systems engineer used models to analyze design constraints and trade-offs. The systems engineer developed test and evaluation parameters. The proposed design was tested against the parameters. The results of the testing and evaluation phase were analyzed to determine the effectiveness of each architecture design. Based on this analysis, the R2C2 Team provided recommendations to the JPO.	**Develop Detailed Security Design** The information systems security engineer analyzed security design constraints and analyzed trade-offs. The information systems security engineer mapped all of the system security requirements to the elements exhaustively. The final detailed security design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.

Table 11: SE and ISSE Phases

5.4 INFORMATION ASSURANCE FOR THE TACTICAL ENVIRONMENT

The R2C2 system is expected to operate in a wide range of environment ranging from a sheltered, air-conditioned hotel room to a rural environment under hostile fire. Information Assurance for system operating in such diverse physical environments is especially challenging. This section highlights some of these specific protection needs. The framework was mapped against the various scenarios for R2C2 operation, namely Pandemic, Disaster Relief, Counterterrorism, Civil Unrest, and Deployment, to determine the protection needs.

5.5 SPECIAL REQUIREMENTS

5.5.1 Wiping Classified Data

The three drivers for tactical data wiping were storage, national level reuse, or multinational reuse of equipment. Tactical data wiping removed residual classified or other sensitive information from any storage media residing in tactical communications or computer equipment. The nature of operation that required the deployment of R2C2 system might transcend different sensitivity and integrity classifications. As such, IA technologies must be available to rapidly and completely remove any sensitive information and ensure that the information would not be recoverable prior to reuse. This would allow the R2C2 system rapidly redeployed at different operation classification level. In scenarios like deployment, counterterrorism and civil unrest, the environments might hostile. As such, the information assurance technologies would include tamper-proof cryptography, programmable cryptographic chips and over-the-air key load and zeroize functions.

5.5.2 Stored Data Protection in a Hostile Environment

Tactical forces faced the possibility of enemy capture or overrun, leading to the seizure of critical, sensitive or classified information. Even in relatively nonhostile environments like Pandemic and Disaster Relief, the R2C2 operators would be charged with the responsibility to maintain the confidentiality, integrity and availability of the information. As such, information assurance technologies like intrusion

detection/prevention, file or media/bulk encryption and zeroization (in case of compromise) should be included. These services should be transparent to the users.

5.5.3 Key Management in a Tactical Environment

Key management played a pivotal role in current information assurance implementation. The overall key management for a tactical communication network involved generation, distribution, and storage of keying materials. These required extensive key management infrastructures (KMI). For purpose of R2C2, it would not be feasible/practical for two-person operators to manage this extensive infrastructure. As such, remote key management mechanisms, like remote rekey, were essential to eliminate the need for large COMSEC logistics in the field. Mechanisms like over-the-air rekey (OTAR), over-the-air zeroize (OTAZ) and over-the-air transfer (OTAT) of keys enable reaction for key compromise to ensure continual provision of services. There must be an automated process for conducting the above mechanisms.

5.5.4 Network Mobility/Dynamic Networks

The crux of the R2C2 system lay on the mobility and dynamic connectivity for rapid deployment. However, together with these capabilities spawned a host of vulnerabilities like eavesdropping, spoofing, and denial of service (DoS) attacks. The operator must be capable of seamlessly connected to the network of intent, hence, provision of service. The information assurance must prevent unauthorized access to protected network and provide protection against geo-location by an adversary.

5.5.5 Secure Net Broadcast and Multicast

Tactical communications equipment must allow operators to roam over a wide area and still be able to receive and send secure broadcast and multicast data over the local infrastructure. Even in scenario like the Pandemic and Disaster Relief, it would be required for secure multicast and broadcast in order to exercise principle of least privilege and maintain integrity (and authenticity) of message in order to facilitate rumor suppression.

5.5.6 Low BW Communications

Numerous information assurance technologies were built on high power and BW. In the counterterrorism, deployment and civil unrest scenario, there would be low BW communication to the R2C2 system. These communications were usually operated with little or no assurance. This would potentially compromise the information integrity of R2C2 system. As such, there must be mechanisms to address the information assurance of low BW communications. Potential approaches would include the integration of commercial information assurance tools into tactical systems.

5.5.7 Split-Base Operations

Split-base refers to a situation in which a unit is deployed away from its home base to a forward operating base in or near the battlefield. This cascading concept was evident in the R2C2 architecture. The approach was to operate in the forward position with minimum communications logistics while relying on "home base" infrastructure through communication links. Under such circumstances, the communication linkages would become the bloodlines of the force's capabilities; the force would be dislocated if the linkages were compromised. As such, robust information assurance technologies would be required to ensure the continual provision of services, integrity of information, authenticity of information exchanges. The network-centric configuration approach might address this requirement.

5.5.8 Multilevel Security

The specification of R2C2 system dictated that it must be two-person transportable. This constrained the quantity of physical systems possible. In addition, the system would serve as a trusted subject to negotiate information flow in accordance with security policies. The R2C2 would need to operate in different levels of classification. This would be apparent in the disaster relief and counter-terrorism scenarios, where the system had to interact in a civil-military and coalition fashion. Multilevel systems offered streamlining of device logistics and capability to negotiate communication across different level simultaneously. The potential security violation vis-à-vis the operational requirement to operate in a multilevel system environment

stressed the security system design. The investigation into Multiple Independent Level Security (MILS) with the necessary encryption technologies might address the multilevel security requirement.

5.6 DEFENSE IN DEPTH INTRODUCTION

Defense in Depth is a practical strategy for achieving information assurance in today's highly networked environments. The concept of Defense in Depth is to apply multiple heterogeneous mechanisms deployed in a layered manner across the organization's computing environment so as to protect its data, applications, systems and networks from unauthorized access. Defense in Depth is a best-practice strategy in that it recommends the application of existing techniques and technologies that are currently available to devise a balanced approach to address protection capability, cost, performance and operational considerations.

5.6.1 Adversaries, Motivations, and Classes of Attack

To effectively protect its information and information systems from unauthorized access and attacks, an organization must be able to identify its adversaries, characterize their potential motivations and attack capabilities. From the outcome of the mission analysis conducted for R2C2, the potential adversaries would probably include nation states, insurgents, terrorists and hackers. Their main motivation would be reconnaissance and intelligence gathering so as to devise the appropriate countermeasures for the various planned missions. The IATF considered five classes of attacks, which could be summarized in Table 12.[106]

[106] National Security Agency, "Information Assurance Technical Framework (IATF)," Release 3.1, September 2002, Chapter 2, p. 5.

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can also result in disclosure of information or data files to an attacker without the consent or knowledge of the user.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-In	Close-in attack is characterized by individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information.
Insider	Insider attacks can be malicious or non-malicious. Malicious insiders intentionally eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as "getting the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

Table 12: Classes of Attack

It was assumed that the threats induced by the insider and distribution attacks, shown in Table 12 in italics, would be mitigated by through personnel security screening and an existing secured distribution channel respectively. As such, the focus is on the first three classes of attacks when devising an appropriate suite of security protection measures for R2C2.

5.6.2 People, Technology, Operations

Information Assurance is achieved when there is confidence that the confidentiality, integrity, availability and authenticity of the information is attained, and is protected against attacks by the protection mechanisms that are in place. To fully realize the Defense in Depth strategy, the achievement of Information Assurance would require a balanced focus of three primary elements, namely, people, technology, and operations, as depicted in Figure 19.

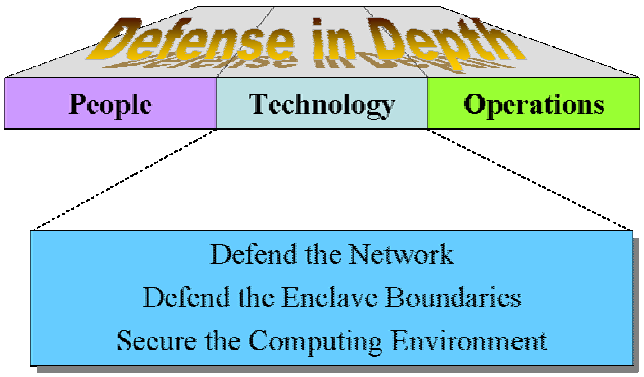


Figure 19: Defense in Depth Strategy[107]

It was the deliberate intention of R2C2 to focus on the technology aspects of providing Defense in Depth, which was also in line with the focus of the IATF. The technology focus areas are further categorized into 1. Defend the Network, 2. Defend the Enclave Boundaries, and 3. Secure the Computing Environment, details of which would be covered in the subsequent sections.

5.7 DEFENDING THE NETWORK

Networks are mechanisms for the transport of data between users. They must be protected against data interception, as well as DoS attacks that could bring information flow to a halt. Such protection will encompass user, control and management traffic.

The type of communications technologies used in the R2C2 architectures includes satellite links, IEEE802.11, IEEE802.16, military links as well as Iridium phones. All these communications links, seen in Figure 20, will have to be protected.

[107] National Security Agency, "Information Assurance Technical Framework (IATF)," Release 3.1, September 2002, Chapter 2, p. 7.

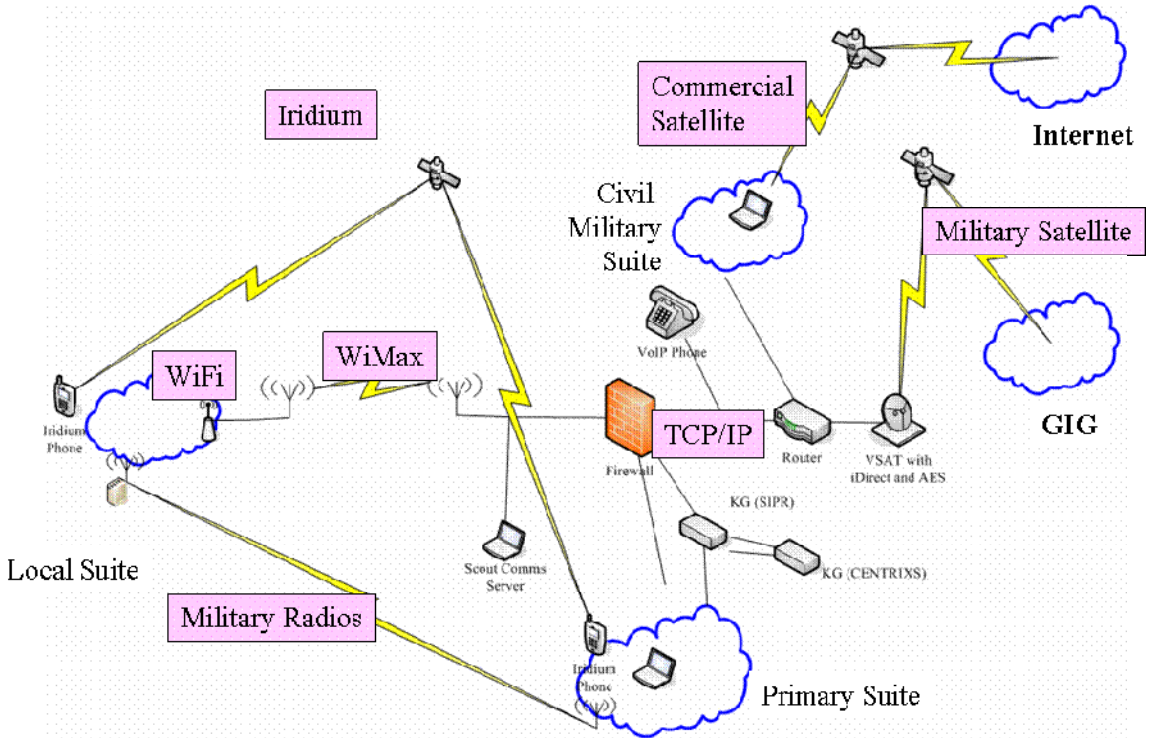


Figure 20: R2C2 Communication Links

Threats to the network include interception of content (full awareness of all communications), interception of IP headers (traffic analysis), spoofing (steal data or inject false data), and jamming (denial of service).

Security requirements for the network comprise access control, authentication, availability, confidentiality, integrity, and nonrepudiation. The general approach towards information assurance in the network will be multiple layers of encryption, and strong network identification and authentication. This will include the use of Teleport sites and NSA approved (e.g., Type 1) encryptors to protect classified data transported over the network. In order to ensure network availability, there will be a need to utilize approved mechanisms that ensure the positive control of network elements, Public Key Infrastructure (PKI) enabled authentication and access control for remote management of all critical network elements, and authentication and integrity protection for all network management transactions.

A combination of software (shown in blue in Figure 21) and hardware (shown above in black) mechanisms would be useful in defending the network at the various layers. To secure datalink traffic, Advanced Encryption Standard (AES) would be

employed, as well as hardware-based SecNet-11 devices. At the network layer, Viasat KG-250 and TACLANE Type 1 network encryptors (hardware-based) would provide another layer of protection. Yet another layer of tunnelling protection would be employed at the application layer, through the use of Secure Shell (SSH) and Secure Socket Layer (SSL).

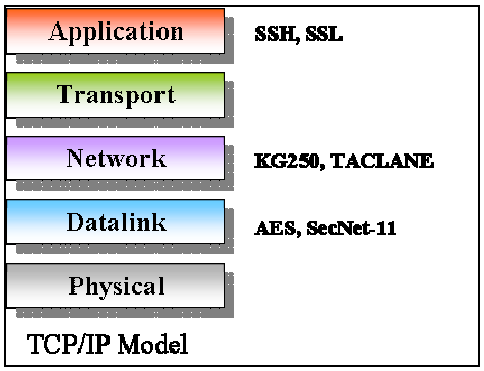


Figure 21: Defending the Network at Various Layers

In the future, SecNet-54 devices could be used instead of the SecNet-11 ones, allowing greater data communications throughput over the WLAN at IEEE802.11 a/b/g (SecNet-11 only operates at IEEE802.11b). NSA certification is expected in fall 2006.

5.8 DEFEND THE ENCLAVE BOUNDARY/EXTERNAL CONNECTIONS

This section addresses the role of IA technologies in providing protection for the enclave. An enclave is an environment under the control of a single authority with personnel and physical security measures. It is an important component of the defense-in-depth strategy for IA. There are three identified enclave boundaries in the R2C2 system which consists of three suites, namely the Primary Suite (PS), the Local Suite (LS), and the Civil/Military Suite. Each suite is encompassed by an enclave. Each suite either has a network connection to another suite or has an external connection to SIPRNET, NIPRNET, CENTRIXS, or the Internet. Each of these enclaves are governed by its own unique security policy.

The defense focus of the enclave boundary is on the effective control and monitoring of data flow in and out of these enclaves. Devices such as firewalls, guards, intrusion detection systems (IDS), network vulnerability scanning tools and virus detectors will be deployed in the R2C2 LAN for enclave boundary protection and

monitoring. Their main purpose is to protect the inside from the outside by access controlling as well as to detect and respond to malicious network activities within the enclave. The following includes some of the recommendations in support to the IA strategy for secure enclaves and between secure enclaves and external systems.

5.8.1 Firewalls

Firewall is an important enclave boundary protection mechanism that prevents against external attacks such as unauthorized extraction, modification, or deletion of the data, denial-of service, and theft of resources or service. A firewall will be deployed in the R2C2 system to restrict incoming and outgoing network connections between the PS and the LS as well as between these two suite and external connections such as the Internet and RCC. It will be placed in between the PS, the LS network and the external network, see Figure 22. The main concern here is to protect the R2C2 laptops and its data in the PS from the external connections.

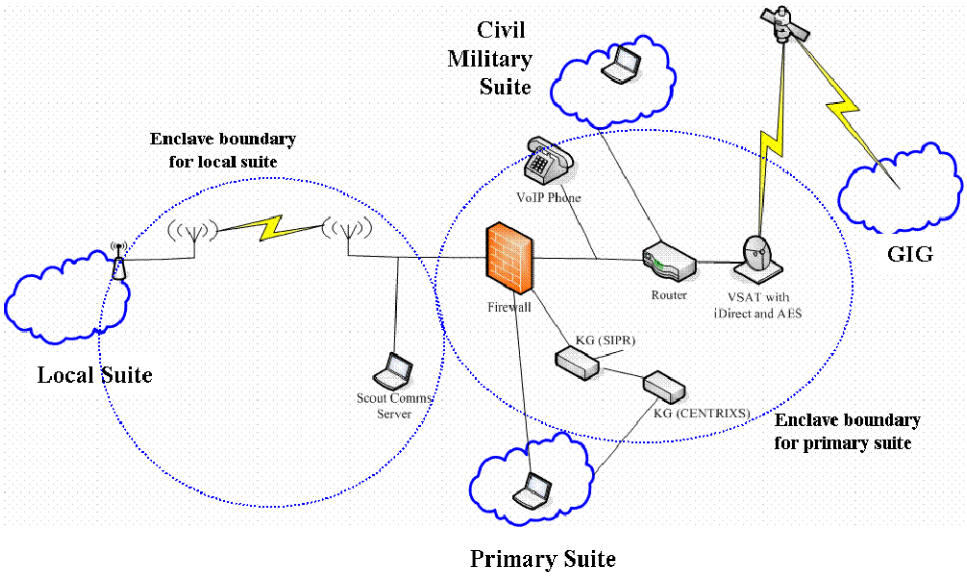


Figure 22: R2C2 Enclave Boundaries

The features of the firewall should be comprehensive enough to provide the adequate protection for R2C2. The firewall should provide access control/filtering capabilities such as restriction of sources, destinations and services, blocking of dangerous protocols, restriction of executable services and download capabilities, and use of internal access control lists. It should also include identification and authentication

mechanisms to authenticate outsiders to the boundary points. Any external users from the LS and the RCC who require access to the PS shall be authenticated. The firewall should also hide the PS and LS networks using network address translation, audit the activities within the networks and scan for malicious software from every incoming external connections from RCC and the Internet.

For more cost effectiveness and better maintainability, it is recommended to have a hardware firewall deployed for the R2C2 as compared to installing software firewalls in each R2C2 laptops. This option will provide a single point-of-control and satisfies the feature requirements listed above.

There are three general types of firewalls, namely packet filtering, stateful packet filtering and application gateway. As there will not be any services such as FTP, DNS, SMTP, etc. provided by the R2C2 laptops, a firewall equipped with stateful packet filtering capabilities would be sufficient for the R2C2 environment. It has the ability to accept or reject packets based on the header information as well as the data of the packet where the application protocol appears. In addition, it dynamically maintains the state and context information about the previous packets.

5.8.2 Guards

A guard enables data exchange between two or more networks operating with different classes of security levels. The main purpose of a guard is to provide data sanitization and separation where various processing, filtering and blocking techniques are involved. It may also involve human review of the data flow. The guard may consist of both hardware and software components to provide secure connection between the enclave boundaries.

The R2C2 scouts at the local suite collects raw data such as digital pictures and video clips and sends back to the PS laptops in the primary suite for processing and analysis. As the information involved in the primary suite is of higher security classification, the scouts will not be allowed to directly offload the collected data into the PS laptops. Instead, an external server, known as the scout communications server will be deployed in between the scouts' collection equipment and the PS laptops (see Figure 22). This external server will facilitate the scouts offloading the collected

raw data meant for the PS operators. The PS operators will then access this external server via the firewall to download the raw data. Human decision making is required from the PS operators in deciding what data to pull from the scout communications server into the higher level of security classification network. The scout communications server performs more like a data clearing house than a guard. However, similar to what a guard aims to achieve, the deployment of the scout communications server between the scouts and the PS operators aids to provide a controlled information flow from a lower security classification network to a higher one. The scout communications server is deployed outside the PS to prevent the R2C2 scouts from introducing malicious files into the PS in the process of the data uploading.

Some of the security features identified for this guard includes the use of identification and authentication mechanisms which only allows authorized users to send or receive the data, auditing all offloading or downloading activities and data encryption capabilities.

5.8.3 Network Monitoring within Enclave Boundaries and External Connections

IDS will be deployed in the R2C2 environment to provide the network monitoring capabilities within the enclave boundaries. It provides detection and response capabilities to mitigate any network attacks. It complements the firewall in the defense-in-depth strategy by detecting all kinds of malicious network traffic and computer activities within the enclave where most firewalls are incapable of.

A host-based IDS is recommended for the R2C2 operating environment and will be installed in each PS laptop. There are several factors contributing to the recommendation. First, software-based IDS would help to reduce the number of heavy equipment the R2C2 crew has to carry and deploy at the operating theater. Secondly, as the number of laptops to be protected within the enclaves is small, it is more cost-effective and economical to use a host-based solution. Furthermore, the specialist knowledge required to operate and utilize a network-based IDS is more demanding. In a tactical environment like R2C2, minimum training for the R2C2 crew to use the equipment would be the preferred option. Finally, another layered defense of network intrusion detection would probably come from the external connection to RCC itself

where it is assumed that more sophisticated network IDS are deployed at the other end. In addition, a host-based IDS with signature-based detection is proposed as it requires less configuration and specialist knowledge than one based on anomaly detection.

5.8.4 Network Scanners within Enclave Boundaries

In addition to the networking monitoring capability provided by the IDS, another type of capability, provided by the network vulnerability scanner may be implemented to improve the overall security posture of the enclave boundary. While the former deals with the "cure" part, the latter provides the preventive measures. It typically operates either periodically or even at the request of the operator on an ad-hoc basis to examine systems for known vulnerabilities that can be exploited by the adversary.

However, there will not be any network vulnerability scanners deployed physically in the R2C2 system. Instead, since the R2C2 has an external connection to the RCC, it is assumed that the RCC has the supporting infrastructure to provide the network vulnerability scanning capability. The network vulnerability scanners at the higher command end would provide features such as comprehensive vulnerability identification and analysis, password cracking and risk analysis.

5.8.5 Malicious Code Protection

Malicious codes can destroy data through network connections if they are allowed to go beyond the network access points or through the individual workstations. Malicious code scanning technologies prevent and/or remove most types of malicious code such as viruses, worms, logic bombs and Trojan horses. The four separate levels of defense against malicious code should be adopted as far as possible for the R2C2 laptops. They are the implementation of pre-infection prevention, infection prevention, infection detection, and infection identification. Antivirus software and spyware programs approved by DoD should be installed at the R2C2 laptops to provide adequate malicious code protection. In addition, the firewall deployed at the network access points offers another layered defense by scanning malicious code embedded in the packets from incoming traffic. Lastly, similar to the network vulnerability scanning approach, it is assumed that the RCC provides the three layers of defense against malicious code.

5.9 SECURE THE COMPUTING ENVIRONMENT INTRODUCTION

Securing the computing environment focused on the use of IA technologies to provide for the confidentiality, integrity, availability, and authenticity of information as it enters, exits, or resides in clients or servers. Clients are typically end-user workstations which include desktops, laptops and peripheral devices. Servers host services that are accessible by clients, and range from Web, applications, and files, to databases and email services. Defending the computing hardware and software of both clients and servers from attack could be the first line of defense against the malicious insider, or it could be the last line of defense against the outsider who penetrates the boundary defenses. In either case, securing the computing environment is necessary to establish an adequate IA posture.

5.9.1 Authentication, Authorization, and Auditing

Identification and Authentication (I&A) is the process of recognizing and verifying the identity of a user who is trying to gain access to protected resources. I&A is fundamental for access control implementations, permitting authorized users and denying unauthorized users; as well as a means of providing accountability through identity-based auditing. The authentication phase could be performed in three different ways: 1) something the user knows (such as a password or pin); 2) something the user has (e.g., an identification card or hardware token); or 3) something the user is (biometrics). A combination of these mechanisms could also be used to achieve strong authentication. Access control is the process of granting access to protected resources only to authorized users, and denying unauthorized users such access. Access control could only be achieved upon successful I&A. Auditing is the process of logging information system activities to facilitate subsequent analysis in support of anomaly detection and information forensics activities. Coupled with I&A, the presence of auditing would encourage user accountability and act as a deterrent to potential malicious activities. Henceforth, the use of I&A, access control mechanisms and auditing would provide the confidentiality, integrity and authenticity of the information.

5.9.2 File Encryption

Data confidentiality means that information is not disclosed to unauthorized users. Access control mechanisms could support data confidentiality by controlling access to protected resources. When the application is not executing, data in storage is vulnerable without the underlying OS or application controlling access. This is where encryption plays a vital role in ensuring data confidentiality.

File encryption protects information in the computer by encrypting the stored information. There are two basic types of file encryption, namely, one in which the user selects specific files to encrypt and one that automatically encrypts all information that is currently not being processed. The former could be used to securely transfer information between systems or to protect information stored on removable media. The latter is used to protect all files stored within the computer system, and with the incorporation of a cryptographic checksum, it could be used to provide both confidentiality and integrity of the contents within the data storage media.

5.9.3 Operating Systems

The IA strategy promulgated by the IATF is to provide a centrally managed, securable, and securely configured operating system foundation. As a baseline, it is recommended that the choice of operating systems be made from those having obtained EAL4+,[108] namely, Microsoft Windows 2003 Server, Windows XP, and Sun Solaris 9. System administrators should ensure that the initial configuration is secure, and enable only required services. Thereafter, they should make a consistent effort to ensure that vendor updates and patches are maintained, subsequent configuration changes maintain or improve security, and that systems are audited on a regular basis to ensure that the configuration remain secure.

---

[108] An **Evaluation Assurance Level** (EAL) is an assurance requirement as defined by Common Criteria, an international standard in effect since 1999, to replace the ratings found in Orange Book that were set by National Computer Security Center. The increasing assurance levels define increasing assurance requirements in computer systems.

5.8.4 Host-Based Detect and Respond Capabilities

The host computing environment is the last line of defense in the Defense-in-Depth strategy. There is a need to equip both clients and servers with the capability to detect and respond effectively to mitigate the effects of attacks that do penetrate the perimeter defenses. The detect capability measures the effectiveness of the deployed protection mechanisms, whereas the respond capability could potentially improve the protection measures being put in place. Figure 23 summarizes the respective protection mechanisms that are captured under the host-based detect and respond capabilities.

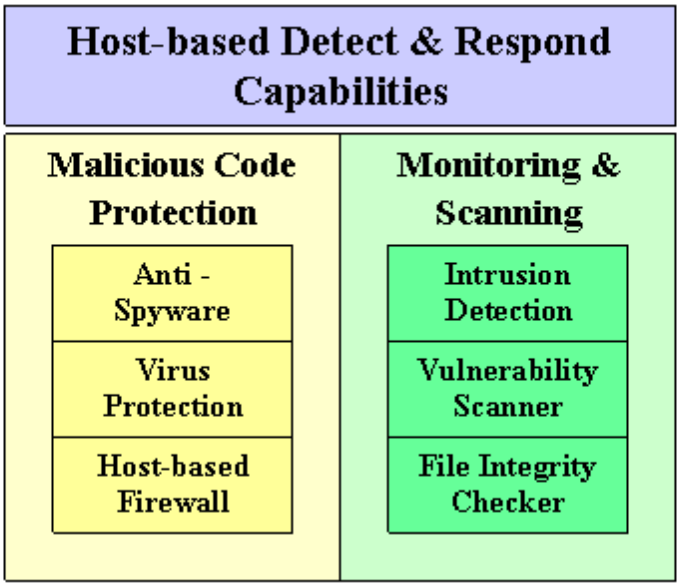


Figure 23: Host-Based Detect and Respond Capabilities

5.10 MULTI-LEVEL SECURITY (MLS) RESEARCH

MLS has many implications on the R2C2 system. It is particularly well-suited for R2C2 operating environment because the R2C2 teams are expected to work closely with Coalition forces and Civil-Military agencies, and MLS directly supports this requirement by allowing information of different classifications to coexist in one system. MLS provides assurance that adequate separation between the different classifications of information is enforced. Different parties can potentially make use of the same terminal and log in at different session levels to access information authorized for them. The

ability to make use of the same terminal provides potential weight saving opportunities, greater flexibility in deployment as well as easier logistics support for the system. As such a portable MLS would be a recommended upgrade option for the next generation of R2C2.

There are currently two broad areas of development in the field of MLS research. One is the development of a highly trusted Operating System that is able to enforce the desired policy via a Separation Kernel. The Naval Postgraduate School has ongoing research on in this area. The other development is MILS. In contrast to MLS, where information of different classifications can coexist, MILS takes a different approach by isolating each level of information within its own single-level environment. The University of Idaho[109] is one of the academic institutions active in this area of research.

5.11 CONCLUSION

The security architecture for the R2C2 system has been incorporated into the system design. A Defense-in-Depth strategy was adopted to ensure the confidentiality, integrity, and availability of information in the R2C2 system. Security architecture was proposed to protect the various enclaves. A brief update on the current areas of research on MLS was included for consideration for future upgrades.

[109] Carol Taylor and Jim Alves-Foss, "MILS Multiple Independent Levels of Security," University of Idaho, http://www.acsac.org/2005/case/thu-130-taylor.pdf. Last accessed in May 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

6.0 MODELING

6.1 INTRODUCTION AND RATIONALE

In this capstone project, there were several opportunities and avenues for exploring architecture performance through modeling and simulation. The team determined that through modeling it was possible to gain valuable insights to assist us in making our final selection of architectures. The results gained from the models complemented architecture design decisions and provided credibility to their analysis.

Early in the modeling process, it was decided that the simulation efforts would be specific and concise, rather than focusing on modeling the system as a whole. While initial thoughts for modeling centered on completing a full-system model, it was determined that not enough information existed on the hardware and software performance characteristics. The team needed modeling to help *select* a final architecture, not to *test* that final architecture. While a full-system model would have been the preferred modeling solution, it was deemed infeasible considering the available software tools provided, and the team's limited knowledge of the hardware components contained in the architecture.

The selection of what to model then shifted to answering specific questions that could aid the team in its architecture selection. The first of these questions was "Why are we modeling?" The team did not create a model because it has historically been a part of integrated projects, but rather because there were specific things that were important to know in order to make a final architecture decision. The team's modeling efforts then set out to address three goals.

First, the models sought to test assumptions developed within the CONOPS and scenarios. As the CONOPS for the scenarios were created by extrapolating from research into similar missions as well as personal operational experiences, it was uncertain to what extent the impact of their assumptions would have on the selection of a final architecture.

Second, modeling was important because the modeling results weighed heavily in the selection of a final architecture, and helped to contribute to further analytical methods (such as the selection of questions in the AHP questionnaire). By gaining insight in the

performance of various architecture choices, it was possible to see what effect that they would have on key system drivers such as weight and throughput.

The third reason that the project team found that the use of modeling tools was justified was that there were specific questions that needed to be answered where there were no clearly apparent solutions. Our approach to these questions involved analyzing the differences between architectures using key factors such as: transmission time, bandwidth utilization, and system weight. Outputs from this process can then be used to select the preferred architecture for given scenarios.

6.2 QUESTIONS ASKED

"*What value is there in a dedicated data link between scouts and the R2C2?*"

It was unknown if there was reasonable justification to include a wireless data link between the scouts in the field and the R2C2 Primary Suite. Timely data transmission was not a consistently critical element of each scenario, and bringing along a dedicated package would incur a significant amount of additional gear. The answer to this question was largely in understanding the necessary requirements that the CONOPS had on the architecture.

"*Is a separate Civil/Military system warranted, or is there excess capacity at the Primary Suite?*"

The need for a separate Civil/Military System was largely dependent on understanding the needs of the Primary Suite users. In the case that the users of the Primary Suite are not consistently stressing the communication link, then it would be unnecessary to include a separate Civil/Military System in the final architectures. As in the previous question, modeling was also a way to understand the effect that the developed CONOPS had on the selection of architectures.

"*Does our choice of architecture still fit the two-person transportable requirement?*"

The last of the three important questions we sought to answer involved learning how our architectures fit within the transportability requirements in the CPD and BAA.

Any added weight will come at the expense of transportability, so there was a critical eye on any additional weight that might break established limits.

6.3 CHOICE OF TOOLS

Several software tools were considered or used in the completion of this project. The most prominently utilized piece of software was EXTEND by Imagine That Inc. EXTEND was used because it was available within the Wayne E. Meyer Institute of Systems Engineering computer labs and the team members had some degree of familiarity with it due to a course in simulation software. While EXTEND does not have the same level of granularity with respect to communication links found in advanced software packages such as OPNET or QualNet, its object-oriented interface, as well as its ease of rapid model fabrication, made it the overall choice.

Both OPNET and QualNet were originally considered to help model aspects of the system, however, due to their complexity, it was unclear whether they had the ability to specifically address the project team's questions within the limited timeframe of the integrated project.

Additionally, Microsoft Excel was used as a software tool for the purposes of weight tradeoff studies and mathematical comparisons.

6.4 PRIMARY SUITE RESULTS

The selection of a Primary Suite was driven by two key factors. The Primary Suite must meet the technical and functional requirements outlined in the CPD, as well as maintain the necessary two-person transportable objective. As seen Chapter 4.0, System Architecture Design, five satellite terminals were considered for inclusion in the Primary Suite. Of those five, three were able to meet the multiband requirement as well as the bandwidth threshold. Table 13 shows the results of market research and analysis. By evaluating system characteristics, it was possible to narrow down the selection to two possible candidates.

Sat System	Bands			Weight		Transmit Rate	Receive Rate	License	Power Consumption
	X	*Ku*	*Ka*	*lbs*	*# of cases*	*Mbps*	*Mbps*		*W AC*
Norsat Globetrekker	optional	yes	optional	<50	1	4	4	Pending	480
Norsat U.P. 5200	optional	yes	optional	46/46	2	8.448	8.448	Pending	480
Swe-dish IPT-i Mil Suitcase	yes	yes	optional	86	1	4	4	Yes	650
TCS DVM-90	no	yes	no	40	1	2.4	2.4	Pending	500
GSI GlobeComm Auto-Explorer (.77m)	no	yes	no	48/50	2	4.2	4.2	Yes Pending	375

Table 13: Available Satellite Terminals and Key Drivers

The final selection was in the SWE-DISH IPT-i Mil Suitcase, as it was appropriately licensed for the satellite constellations needed for the system. Additionally, it was determined that the Norsat Globetrekker should be considered as a possible future alternative. While it does not currently have the necessary transmission licenses, it can fill the same role as the SWE-DISH model at a significantly reduced weight.

Additionally, the Norsat Globetrekker uses significantly less power when transmitting compared to the similar SWE-DISH model. Even without the necessary licenses and certifications, it was determined that it would be wise to keep it considered as an alternative even if it currently may not be a viable option.

Following the results of the market survey and analysis of available satellite terminals, it was possible to create an estimate of overall system weight. Table 14 shows the proposed breakdown by component for each element of the system and their associated weights.

Device	Qty	Weight (lbs)
Laptops & Accessories	5	50
Swe-dish IPT	1	86
Swe-dish cabling/support	1	10
Routers	2	28
Switches	3	33
VTC Gear	1	4
VoIP Phones	2	14
SecNet 11 Access Point	1	2
KG250	2	13
Packaging	3	45
Network Cables	1	5
Generator & Accessories	1	50
Total		340

Table 14: PS Weight

6.5 LOCAL SUITE (LS) RESULTS

Using EXTEND, a model was developed to understand the nature of communications between the scouts and the PS, and to examine how various message delays could have an effect on different mission types. Using inputs developed from the scenarios and CONOPS, it was possible to construct an event-driven model to simulate the transmission of data from scouts in the field back to the R2C2 for analysis.

Figure 24 shows an overview of the model utilized in EXTEND. As scout-produced data was generated on the left side of the model, the time taken to transmit the message was analyzed as the data traveled through the system.

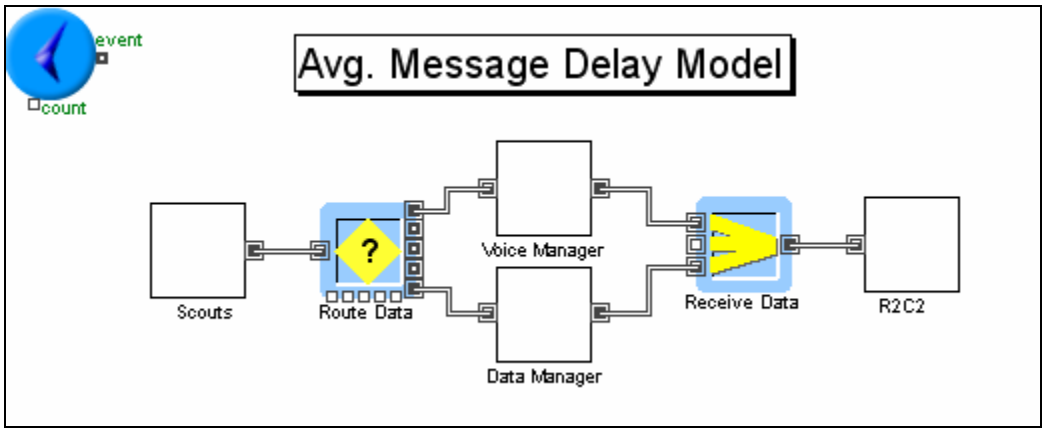


Figure 24: LS EXTEND Model

The developed CONOPS showed that the majority of transmissions from the scouts to the R2C2 were voice in nature (85%), while the remaining transmissions were some form of data (15%). Figure 24 illustrates the breakdown between among the three kinds of data.

This model sought to quantify the delay from the beginning of a transmission to the point where it is fully received by the R2C2 operators. As shown in Figure 25, the majority of communication over the Local Suite was voice-only, and as such, the delay time for voice communications would be exactly as long as it takes to speak the information. However, the delay times for electronic data types (pictures and video) were highly dependent on the existence of a data-link over which to transmit the information. In architectures that include this link (such as 802.16 Wi-Max), the transmission time was a function of point-to-point bandwidth. In architectures without that dedicated link, the "transmission time" is a function of how quickly the data can be physically moved (using available transportation methods) from the field to the R2C2 operators at the PS.

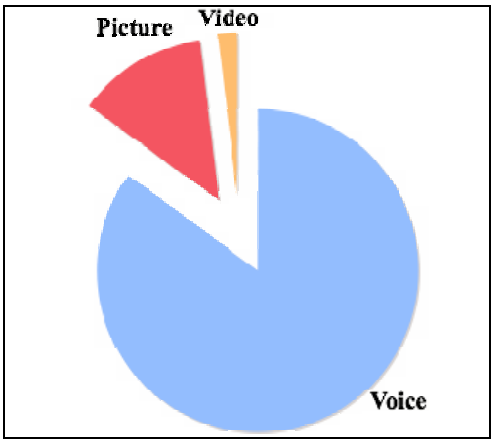


Figure 25: LS Communication Type Breakdown

The CONOPS defined that the users of the LS conduct event triggered and hourly or bihourly communications with the PS to keep the RCC appraised on events. With these CONOPS in mind, and following elements of the El Salvador earthquake scenario, the model showed the significance of bringing along the extra gear to utilize a data link. Figure 26 illustrates the results of the first series of runs by graphing the average amount of time taken to transmit a message from scouts to the R2C2.

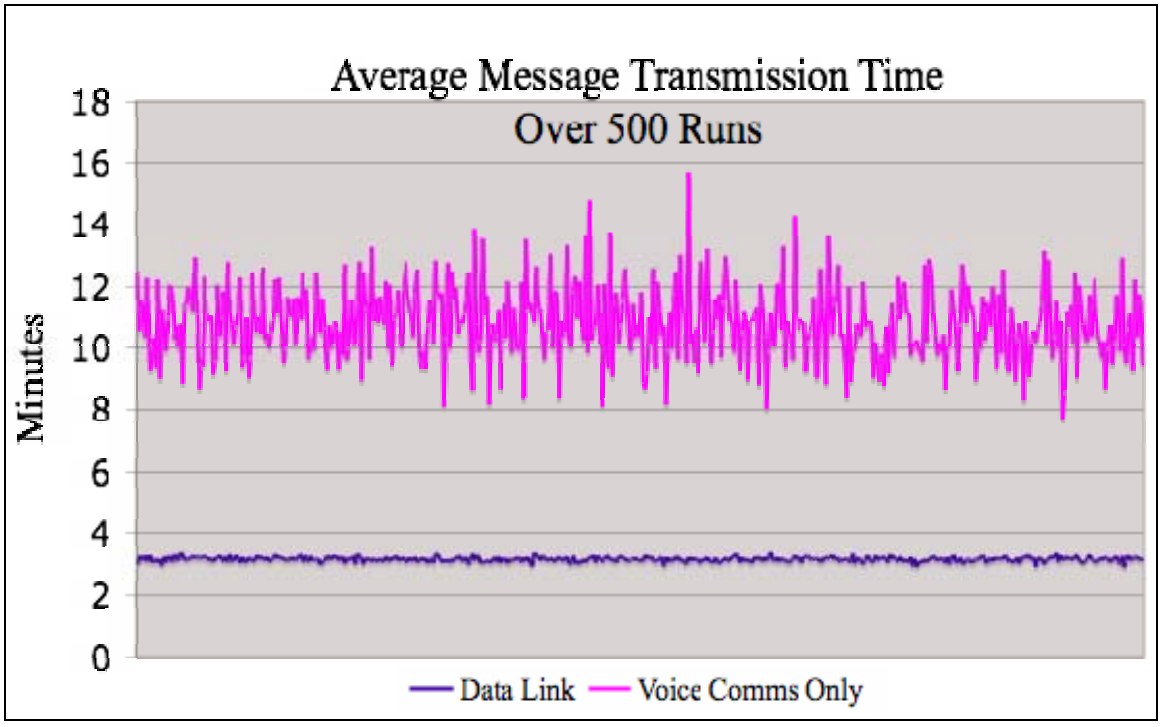


Figure 26: Average Message Delay (Aggregate)

On average, R2C2 systems with a data link were able to transmit a piece of data in 3.1 minutes as opposed to the 11.0 minutes it takes when a link is not present. As noted earlier, the majority of transmissions in both cases were voice-only in nature. Even though data transmission does not occur most of the time, it is an important element in the cycle of time-critical missions. Pictures and video are often used to provide target confirmation in time-critical missions before action is taken. Without an expedient method of transmitting the data back, it may not be able to meet the necessary 30-minute window of decision and action.[110] To further understand the importance of architecture selection on time-critical missions, the model was rerun to specifically look at the delay times in data transmission. Figure 27 illustrates the increased delay when looking at data transmission only.

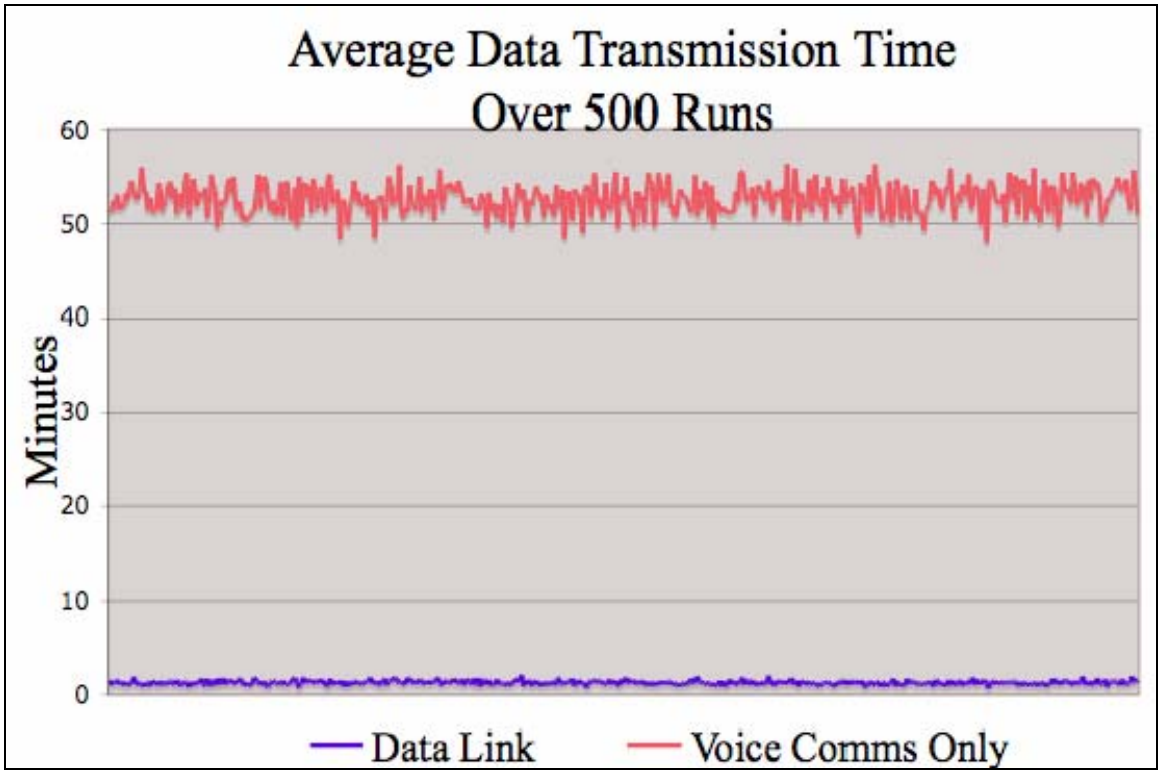


Figure 27: Average Message Delay (Data Only)

The second run of the model focused exclusively on data transmission from the scouts to the R2C2 PS. This graph emphasized that one architecture selection was able to

[110] Jim Morehouse, Brig Gen, USAF, Director of Command and Control DCS, Air and Space Operations, 2002 Time-Critical Targeting Brief, http://www.dtic.mil/ndia/2002interop/morehouse.pdf. Last accessed in June 2006.

meet the 30-minute threshold for time-critical operations. If transmission times were reduced from an average of 55 minutes to an average of 3 minutes, a mission is time-critical in nature and including a data link is likely to meet the requirements, while architectures without one will not.

Tables 15 and 16 each show the estimated gear burden for each scout team. As a result of market research, it was determined that for a primarily voice-only scenario, scouts would only need 2.5 pounds of extra gear for the mission. In time-critical missions concerning a need to meet the 30-minute threshold, scouts would be carrying a total of 51.5 pounds of gear. Despite the fact that there was a significant difference in size between the two packages, this gear would be carried by individual scout teams, and would not count against the two-person transportability requirement for the R2C2 PS.

Device	Quantity	Weight (lbs)
Iridium phone	1	0.5
PDA	1	0.5
Digital camera	1	0.5
Video camera	1	1
Total		**2.5**

Table 15: Scout Gear Breakdown (Voice Only)

Device	Quantity	Weight (lbs)
Voice Comm.	1	2.5
802.16 Transceiver	1	9
Additional Laptop	1	8
Networking Gear/Cables	1	5
802.16 Antenna	1	5
Package	1	3
802.16 Transceiver	1	9
802.16 Antenna	1	5
Cables	1	5
Total		**51.5**

Table 16: Scout Gear Breakdown (Voice and Data)

6.6 CIVIL/MILITARY SUITE (CMS) RESULTS

The Civil/Military Suite was also modeled using the EXTEND simulation software. The goal of this model was to analyze the bandwidth usage of the R2C2 Primary Suite as per the developed CONOPS and determine what excess bandwidth, if any, was available for usage by other entities. The concept of the Civil/Military Suite is that the R2C2 system would facilitate communication for entities other than the Primary Suite operators. For instance, in the El Salvador earthquake scenario, key players in the local government will be without basic communications. The operators of the R2C2 Primary Suite may then act as a lightweight Internet Service Provider until normal communications are restored.

The two options analyzed were a Civil/Military Suite integrated into the Primary Suite and a fully separate system. The decision between the two was based on the idea that while a separate Civil/Military Suite will have a dedicated amount of bandwidth, it may be possible instead to utilize excess capacity in the Primary Suite.

With the Primary Suite leaving sufficient bandwidth for the Civil/Military Suite to utilize, it would be unnecessary to bring along a separate satellite link for their usage.

With scenario and CONOPS input, it was possible to generate an EXTEND model to analyze the usage of the Primary Suite satellite link. What the team wanted to know was the extent of utilization seen on the Primary Suite satellite link. Knowing that the R2C2 CONOPS might not stress the Primary Suite satellite link would allow for an integrated Civil/Military Suite solution.

Figure 28 illustrates the EXTEND model used for this project. Data is generated within the R2C2 block, and by analyzing the type and size of transmission it became possible to estimate the amount of bandwidth that was needed for the system operators.

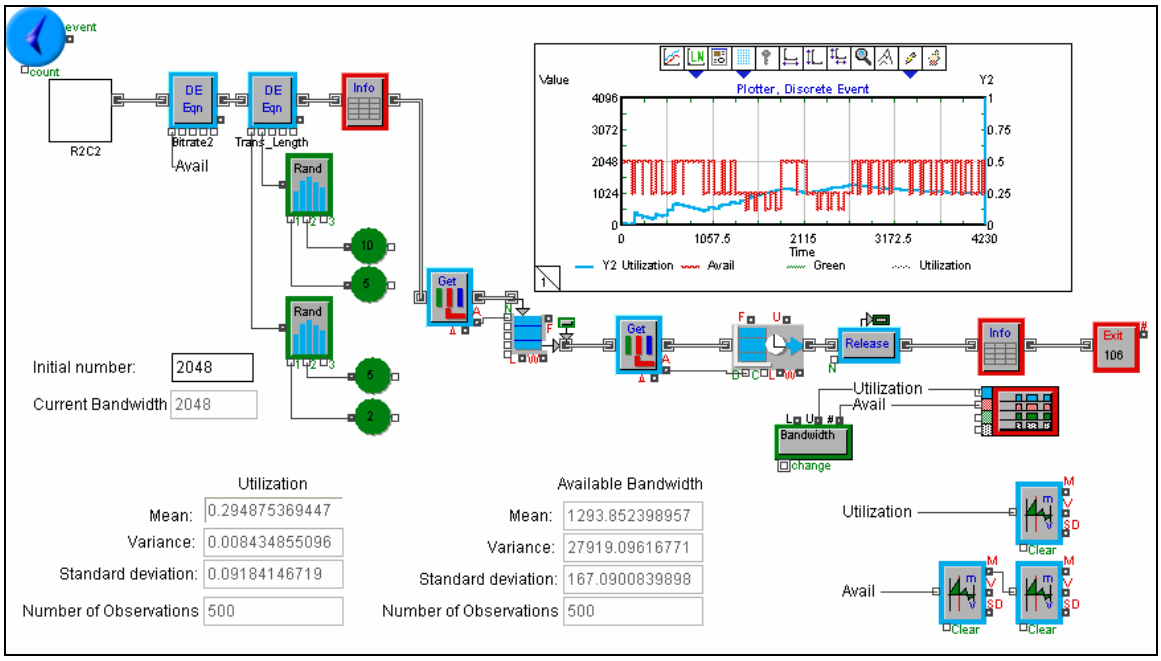


Figure 28: Civil/Military Suite EXTEND Model

The Civil/Military Suite model followed the developed scenarios and CONOPS to see how the assumptions made by the team translated into actual usage figures. The model generated periodic and nonperiodic symmetric communications between the R2C2 and the RCC. System bandwidth was monitored as a resource to provide an understanding of the level of utilization for the duration of the simulation. It was discovered that there was a significant amount of excess bandwidth, as the R2C2 communications were largely periodic in nature. Active transmissions only exist in a

fractional part of the hour, leaving plenty of opportunity for the friendly Civil/Military entities to utilize remaining data resources.

The model was run several times using different bandwidth thresholds (512 kbps, 1,024 kbps, 2,048 kbps, and 4,096 kbps) as seen in Figure 29. Given 24-hours/day operation, it was found that the satellite terminal would remain unused for a significant portion of the day. The result of this model showed two important things: the satellite terminal can either be periodically powered down to save on energy usage, or excess bandwidth could be "donated" for Civil/Military usage. Knowing that the CPD objective for the Primary Suite satellite terminal was 4,096 kbps, it was a safe assumption that there will be a significant bandwidth excess for Civil/Military use. By sharing an existing resource, it would then be unnecessary to bring along a separate Civil/Military Suite.

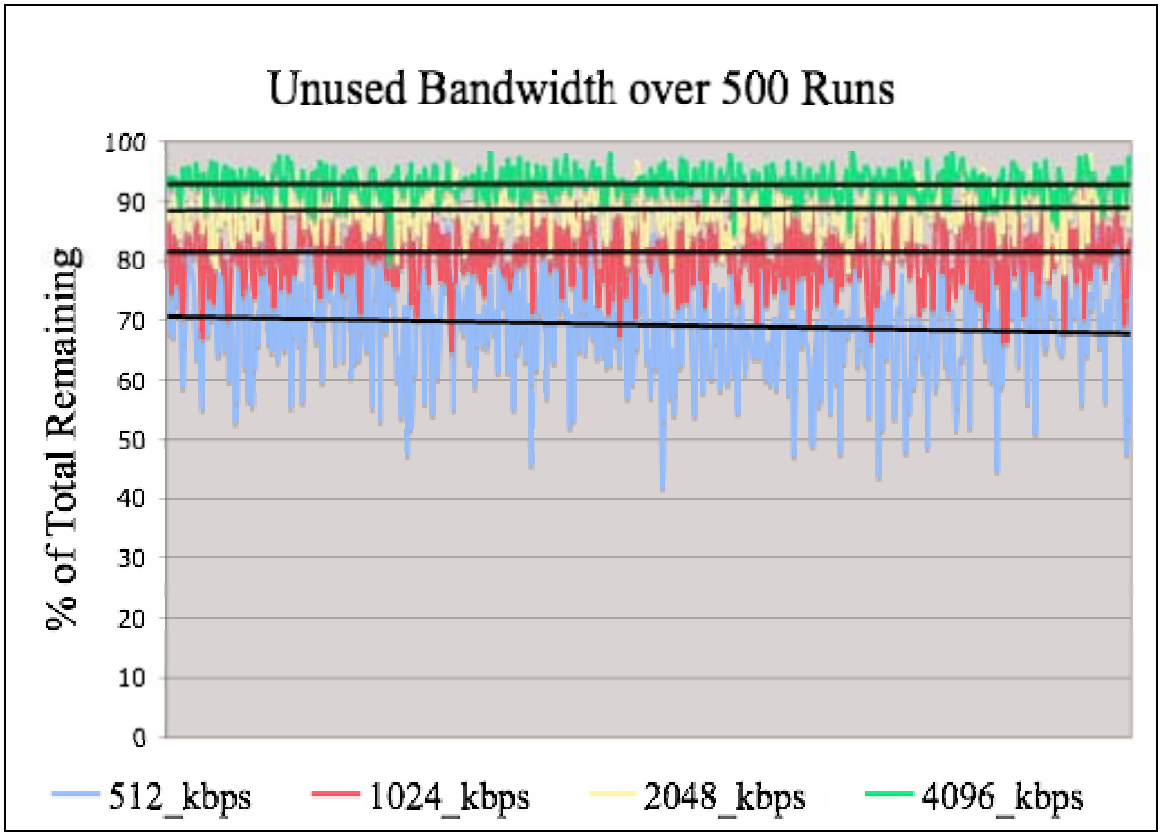


Figure 29: Civil/Military Suite Model Results

6.7 SELECTION OF ARCHITECTURE

The overall choice for system architecture then became dependent on the time-critical nature of the mission. If there was a significant need to meet the 30-minute threshold to confirm and act on information, then it becomes necessary to bring along a separate data link, such as an 802.16 Wi-Max device. Examples of these time-critical missions included the deployment scenario, the counterterrorism scenario, and the Ivory Coast scenario. Conversely, the El Salvador earthquake scenario and the pandemic scenario are examples of normal operations. Time was also important, but it lacked a pressing need to meet the 30-minute, time-critical threshold.

Additionally, when determining the final configuration for the system architecture weight trade-offs were considered because the two-person transportability requirement was a key performance parameter for the program office. As seen in Table 17, there are a series of potential opportunities and risks that can be taken advantage of in the R2C2 system to further reduce its deployed weight.

Risk	Weight Change	System Weight
Lightweight Packaging (less robust and durable)	-27 lbs	313 lbs
Norsat Globetrekker (not yet certified for use)	-36 lbs	304 lbs
Operate Without Generator (power supply uncertain)	-50 lbs	290 lbs
Combined Risk Deductions	-113 lbs	227 lbs

Table 17: Additional Weight Trade-Offs

The first of the possible trade-offs was to use lighter packaging. Initial weight estimates were done using a set of hard plastic suitcases (such as those made by Pelican Cases[111]) with a weight of 15 pounds per case. While these cases were quite durable, they added a significant amount of weight to the system. Alternatively, it may

[111] Pelican Cases, http://www.pelican.com/cases_detail_specs.php?Case=1600. Last accessed in May 2006.

be possible to use lightweight backpacks to carry the gear. McHale backpacks,[112] for instance, manufactures 7,500-cubic inch packs weighing only 6.5 pounds. For less than half the weight of hard cases, it was possible to have similarly sized packaging. While the trade-off was that the system weight is reduced, it was exchanged at the expense of durability.

Another possible trade-off considered was to use the Norsat Globetrekker. Currently, the device is uncertified for use on the constellations necessary for the system, but the licenses are pending. By keeping the Norsat model in mind, it was possible to use it in place of the SWE-DISH model and save 36 pounds of weight for the system.

The third possible trade-off that was identified to reduce the weight of the system was to deploy without an electrical generator. If the deployment location has an operational electrical power system, or if it is an acceptable risk to operate without a steady power source, the weight of the system can further be reduced by about 50 pounds.

6.8 MODEL PROCESS DOCUMENTATION

6.8.1 Local Suite EXTEND Model

The Local Suite model was developed to better understand the importance of a data-link within the R2C2 architecture. The model was comprised of three main components: the scouts (the data generator), the management elements (determine how long data is delayed in transit), and the R2C2 (receive and process data) (see Figure 30).

[112] McHale Backpacks, http://www.mchalepacks.com/packs/detail/MBSuper.htm. Last accessed in May 2006.

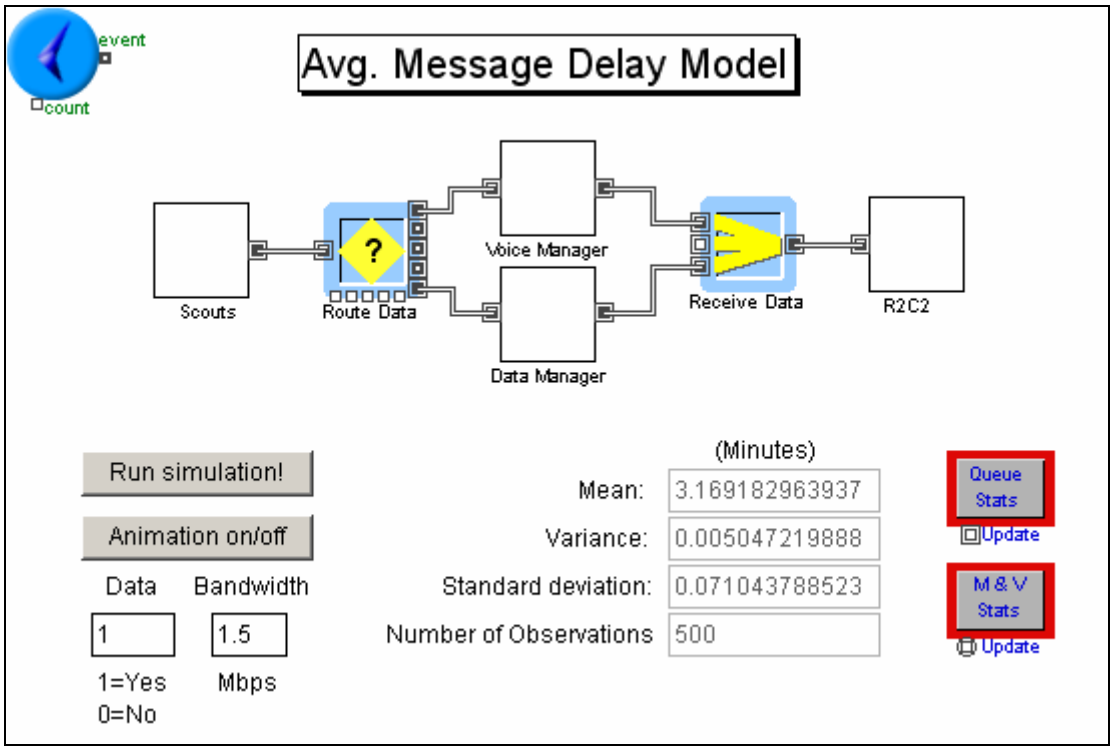


Figure 30: Message Delay Model Overview

The first of the main components was the data generation element. Each scout needed to provide periodic communications to the R2C2 primary system. Figure 31 shows an overview of the data generation process. Each scout was contained within a separate hierarchical block and given an external ID attribute. As scouts generated information, that data was tagged with their ID and merged into a single data stream. If more or less scouts were required in the simulation, hierarchical scout blocks were added or deleted as necessary.

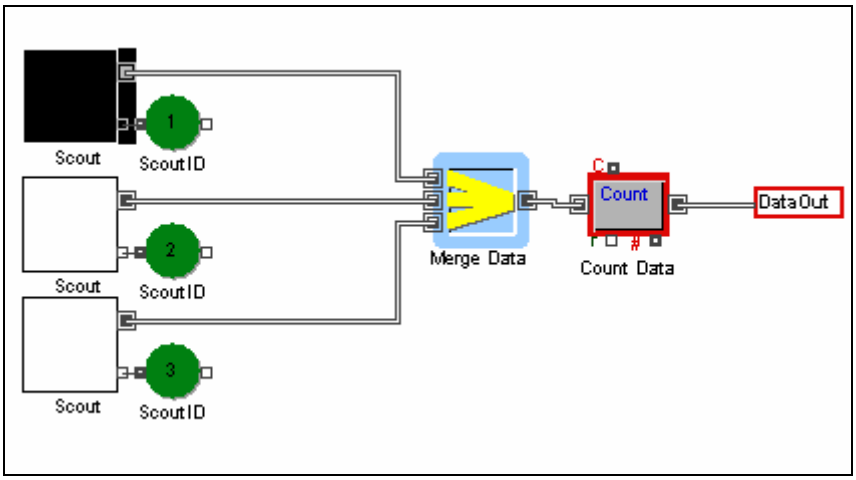


Figure 31: Scout Data Generation Overview

Figure 32 shows the details of data generation within each of the hierarchical scout blocks. The process or data generation started off with a "Program" block that was used to generate a periodic burst of information. The piece of information was then tagged with the scout's ID and a data type. Data typing was done by generating a random number from 1 to 100 and combining it with the information generated from the CONOPS (such as seen in Figure 32). Once the data type was assigned, it was directed through the appropriate path to determine the size of the data. An attribute was then set to represent the size of the information (minutes for voice conversation, megabytes for data) before it left the hierarchical block.

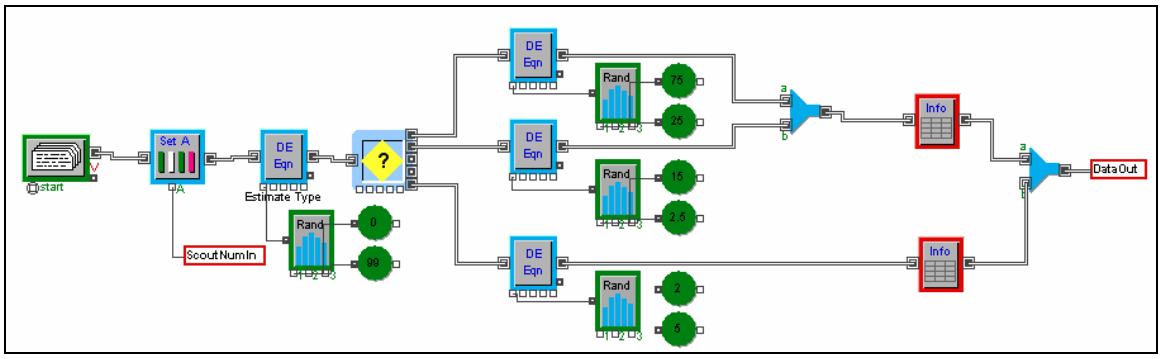


Figure 32: Scout Data Generation

As seen in Figure 30 information was then routed depending on whether it is voice or data. Figure 33 shows how the delay in voice communications was calculated. A piece of information transmitted from the scout by voice was delayed exactly as long as the transmission takes. If, for instance, a report took three minutes to relay, there was

a three-minute delay. The model replicated this by retrieving the message length and delaying it appropriately in the "Activity, Delay" block.

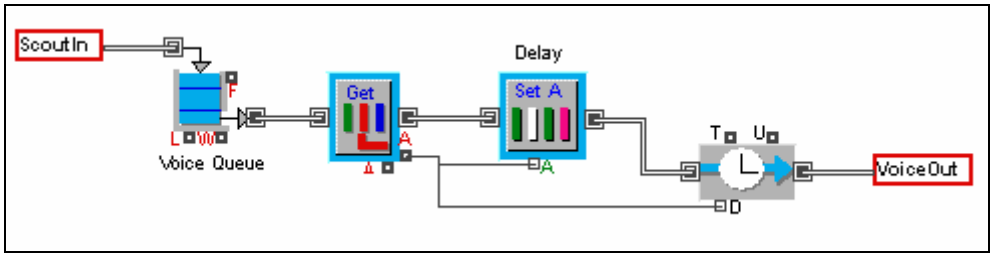


Figure 33: Voice Delay Model

Information that is not voice in nature is routed separately through a Data Delay Model as shown in Figure 34. The Data Delay Model had two different paths, as indicated by the decision block. If data transmission was an option it was added into the Data Queue; otherwise, it was fed into a model to transfer data physically by vehicle.

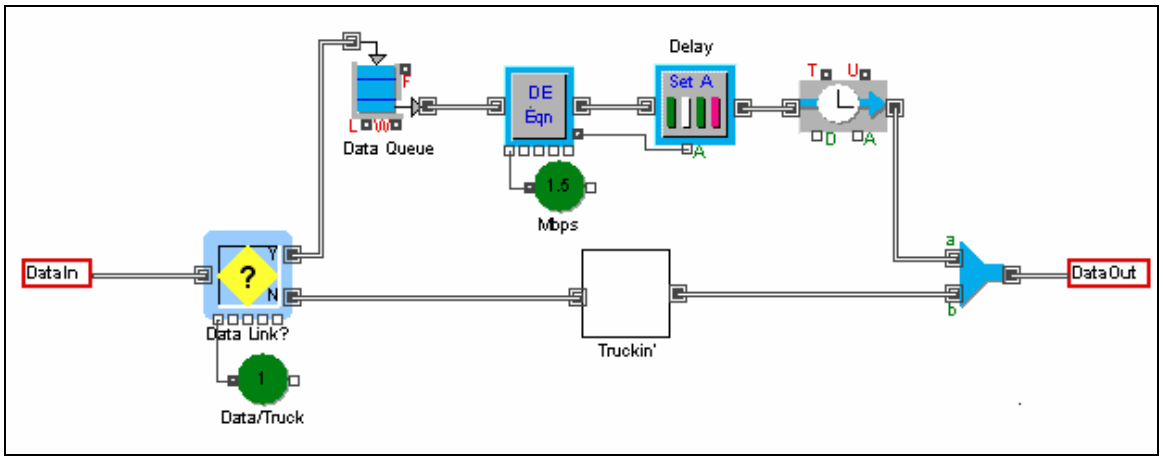


Figure 34: Data Delay Model Overview

The length of delay was determined by dividing the data size (in megabytes) by the available link speed (a variable set in megabytes per second). After delaying the transmission appropriately, data is then forwarded into the R2C2.

Data being transferred physically by vehicle entered the transfer system seen in Figure 35. Figure 35 is the initial breakout of data to be transferred by vehicle. Each scout emplacement had an associated vehicle transmission queue, as represented by the three hierarchical blocks labeled as "Data 'Driven." The scout ID number assigned at the

beginning of the simulation was now used to match outgoing data with the appropriate scout transportation queue.

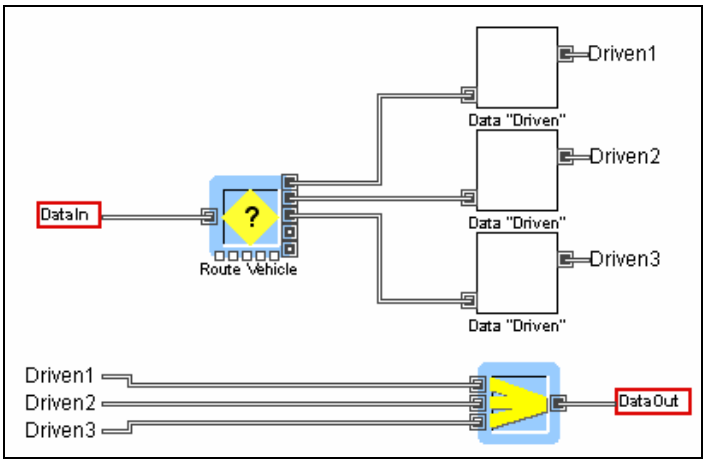


Figure 35: Data Delay Vehicle Overview

Figure 36 shows the details of how a vehicle was used to transfer data. At the start of the simulation a single object (the "truck") was generated. Incoming data to be transmitted waited in a queue for a vehicle to become available. Once a piece of data and a vehicle were paired up, the data was then delayed depending on the distance from the R2C2 and the estimated speed of travel. Additionally, some randomness was added to the transit time to account for variations in road conditions. Once data separated from the vehicle, it arrived at the R2C2.

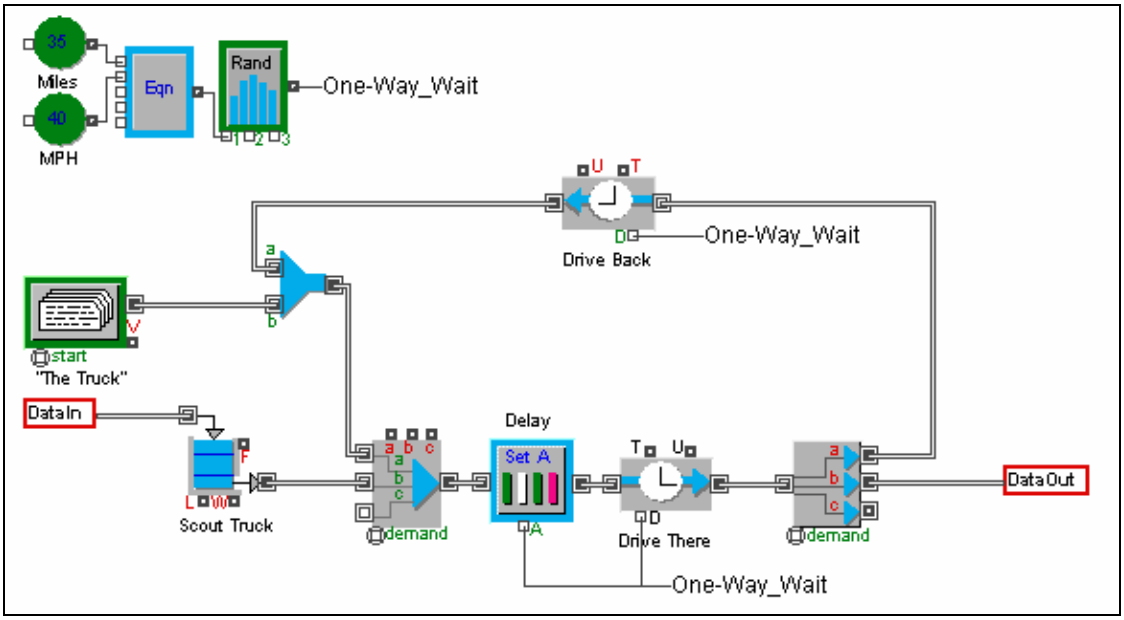


Figure 36: Data Delay by Vehicle

The R2C2 system shown in Figure 37 was the endpoint for the simulation. All pieces of data were queried for delay times, which were then statistically analyzed and recorded in a file. After providing their respective delay times, each data object then exited the model.

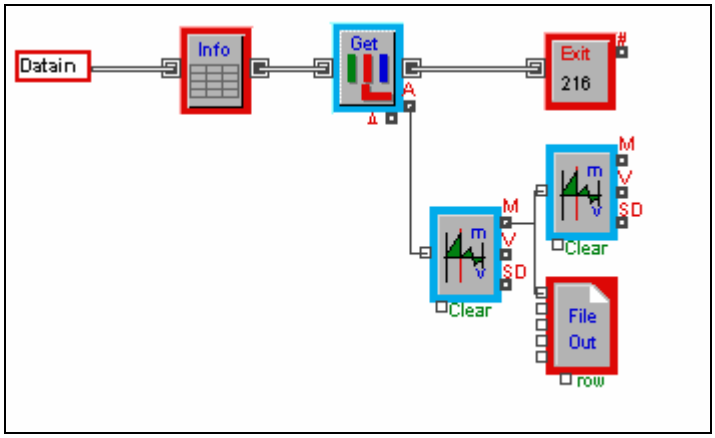


Figure 37: Model Exit and Statistics Recorder

6.8.2 Civil/Military Suite EXTEND Model

The second of the EXTEND models used in this project focused on the analysis of bandwidth usage at the Primary Suite. The EXTEND model sought to simulate periodic and non-periodic transmission from R2C2 operators out to the RCC to understand how the satellite terminal was utilized.

The first part of the model is illustrated in Figure 38. Here there were two different message generation systems. The upper generator created data at periodic intervals, whereas the lower one provided nonperiodic information of varying numbers (multiple messages at once).

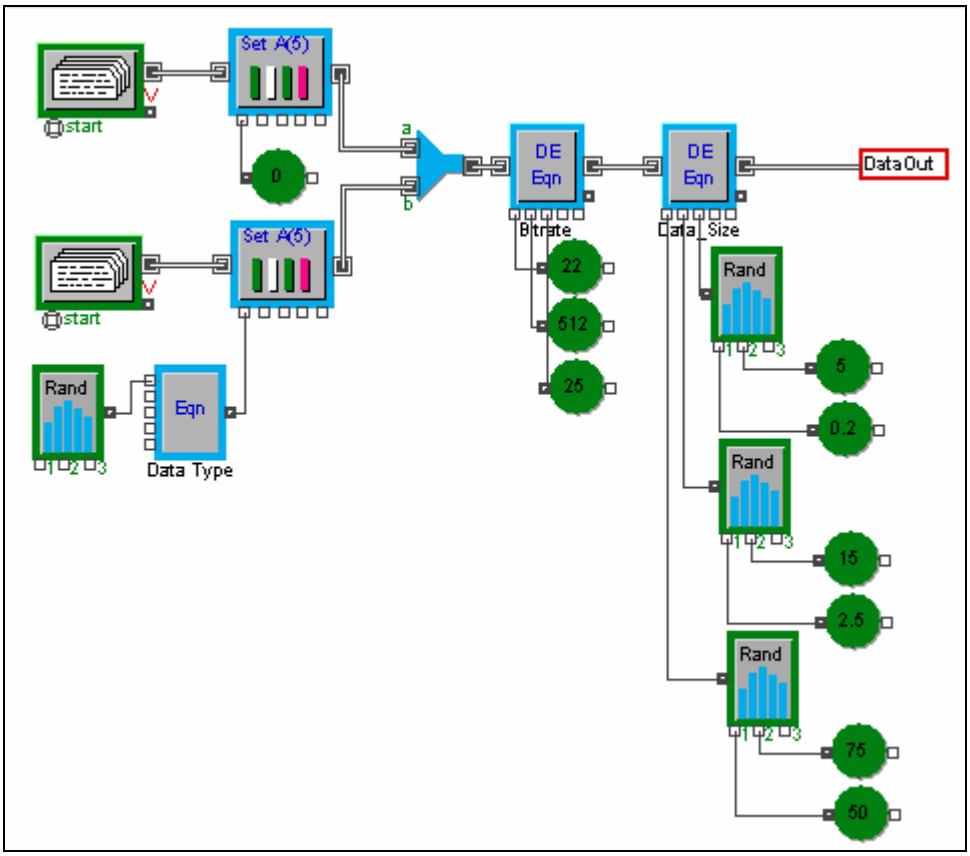


Figure 38: Bandwidth Model Data Generation

Once data was generated, it was assigned a bit rate depending on the nature of communications (voice or video), or a placeholder value for other data types. Depending on the type of data, each piece of information was also assigned a randomized size in megabytes before it entered the remainder of the model. Each parameter, such as the bounds for message size or required bit rates, can be adjusted through the many constants noted by green circles.

The main part of the model is shown in Figure 39. As outgoing data prepares to be transmitted the amount of time necessary to transmit the message was estimated by querying the available system bandwidth. In the event of time-based data communication, such as VTC or VoIP, the overall transmission length was estimated as the length of the communication session.

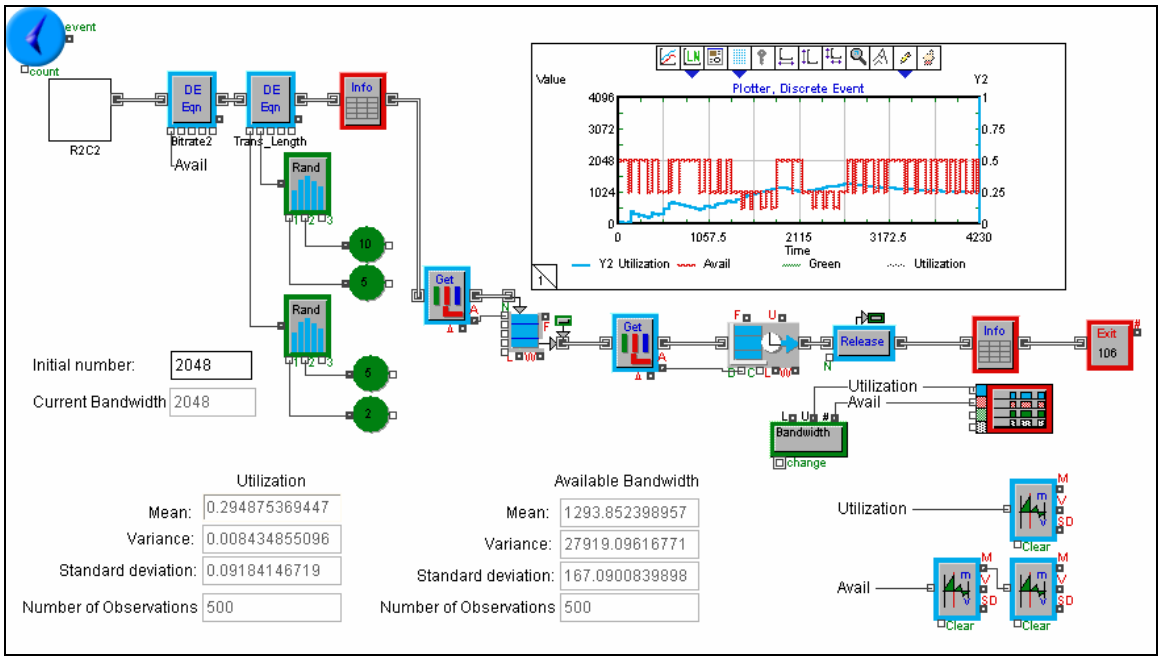


Figure 39: Bandwidth Model Overview

Once a piece of data had an estimated bandwidth usage and transfer time, its bandwidth requirements were deduced from the remaining level and delayed for the appropriate transmission time. As pieces of information exit the model, data about bandwidth usage and availability was recorded and displayed in Figure 39.

The model can be re-run using different bandwidth thresholds by changing the "Initial Number" in the input box to the left of the model. As the model was run, a graph displayed a running view of available bandwidth and average utilization.

6.9 CONCLUSIONS

Through modeling and analysis, the integrated project team was able to determine several key things. First, it would be unnecessary to provide a separate system for Civil/Military use. Modeling showed that the Primary Suite operators do not significantly stress the system, and leave enough excess bandwidth for an integrated Civil/Military Suite. It was also found that the need for the scouts to be supplied with a data link relied heavily on the nature of the mission they intended to accomplish. If the scouts were participating in a time-critical mission where they needed to verify and act on information gathered, then it would be necessary to for them to field a dedicated

data link. If time-critical data management was not a requirement of the mission, then it was possible to field the scouts with a lighter, less capable set of equipment.

Additionally, modeling and analysis has found that there are a series of possible trade-offs that can be done to lighten the overall deployed weight of the R2C2 system. Lightweight packaging in lieu of commonly used durable plastic cases will reduce the system's weight by as much as 27 pounds. The R2C2 could also choose to use the Norsat Globetrekker instead of the currently certified SWE-DISH IPT-I suitcase. While the Norsat model does not currently have the proper licenses for use on satellite constellations, it reduces the system weight by another 36 pounds. The third possible trade-off identified is to deploy without bringing a portable electrical generator. If the system is being used in a region with a reasonably stable power supply, it is possible to save an additional 50 pounds by leaving the generator back home. While the combined weight trade-offs reduce the Primary Suite from 340 pounds to 227 pounds, any weight trade-off selected will better support the two-person transportable requirement.

7.0 SYSTEM ANALYSIS

7.1 INTRODUCTION

For the final phase of the SE process, R2C2 team conducted the system analysis. The time-critical R2C2 architecture from Chapter 6.0 was chosen and various analyses were conducted utilizing the AHP and requirements traffic light comparisons. AHP and the requirements traffic light comparisons provided objective assessment and ranking of three competing alternatives systems: Joint Systems Integration Command Executive Command and Control (JSIC EC2), System Y, and R2C2. In addition to the rankings, AHP served another valuable purpose of providing the criterion priority of rapidly deployable C2 type systems.

7.2 ANALYTIC HIERARCHY PROCESS (AHP)

The AHP is a decision-making process developed by Thomas L. Saaty to help people solve complex problems involving multiple criteria. The prime use of the AHP is the resolution of choice problems in a multicriteria environment.[113] It is a technique that could be used in an individual or group decision-making environment. The application of AHP has proven to be successful in the following areas: selection of alternatives, resource allocation, forecasting, total quality management, and business process reengineering. It is an intuitive method that offers the ability to "mirror" human decision making by structuring issues in a hierarchy from a top-down approach. In other words, it helps to organize data and information into a structured framework proceeding from the goal to objectives to subobjectives. With simple pair-wise comparison judgments throughout the hierarchy, the decision maker would be guided in his analysis to derive the most suitable option among competing alternatives.

AHP's ability to translate a subjective human decision-making process into a quantitative measure also facilitates sensitivity analysis when changes are made to the rating of evaluation criteria. In addition, decision makers can take into consideration

[113] Forman et al., "The Analytic Hierarchy Process – An Exposition," *INFORMS*, Vol. 49, No. 4, 2001.

qualitative attributes such as safety, quality, and ease of operations. Most importantly, AHP provides a clear, transparent, and objective means to arrive at a defensible and credible decision. Hence, the AHP methodology was chosen for the analysis to derive the most preferred system among competing alternatives.

7.2.1 Principles of Analytic Hierarchy Process

The AHP approach to problem solving by logical analysis is based on three principles: the principle of constructing hierarchy, the principle of establishing priorities, and the principle of logical consistency.[114] The principle of constructing hierarchy is based on the natural human ability to breakdown a complex issue into its parts, and these in turn into their subparts, and so on, hierarchically. In this way, large amounts of information can be digested or presented to form an overall picture of the system.

The principle of establishing priorities is again based on the human ability to understand the relationship between various elements of an issue and to rationalize within himself on his preference for one over the other. A relative importance, known as vector of priority, between the various elements in the same level of hierarchy is established by making a pair-wise comparison. Saaty recommended using a scale of 1 to 9 for pair-wise comparison as shown in Table 18.

Intensity of Importance	Definition	Explanation
1	Equal Importance	Two elements contribute equally to the property
3	Moderate importance of one over the other	Experience and judgment slightly favor one element over another
5	Essential or strong importance	Experience and judgment strongly favor one element over another
7	Very strong importance	An element is strongly favored and its dominance is demonstrated in practice
9	Extreme importance	The evidence favoring one element over another is of the highest possible order of affirmation
2,4,6,8	Intermediate values between the two adjacent judgments	Compromise is needed between two judgments
Reciprocals	When activity i compared to j is assigned one of the above numbers, then activity j compared to i is assigned its reciprocal.	
Rationales	Ratios arising from forcing consistency of judgments	

Table 18: The Pair-Wise Comparison Scale[115]

[114] T.L. Saaty, "Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World," RWS Publications, 1990, p. 3.

[115] Ibid., pp. 20-21.

Let c_{ij} denote the value obtained by comparing criterion c_i relative to criterion c_j. If criterion c_j is assessed to be more important than criterion c_i, then the reciprocal of the relevant index value is assigned, and that $c_{ij} = 1/ c_{ji}$. Clearly, all criteria will rank equally when compared to themselves and $c_{ii} = 1$. When the principal of consistency holds true, the condition $c_{jk} = c_{ik} / c_{ij}$ is satisfied. This means that for n criteria, only n (n – 1)/2 comparisons are needed to determine the complete set of pair-wise judgments.

Next, we denote the pair-wise comparison matrix A and the vector of priority w such that each element $c_{ij} = w_i/w_j$ for all i and j. Given a perfectly consistent matrix A, if we post multiply A by the column vector w, the relationship between A and w could be established.

$$Aw = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{pmatrix} = \begin{pmatrix} nw_1 \\ nw_2 \\ . \\ . \\ . \\ nw_n \end{pmatrix} = n\, w$$

This relationship is given by (A – n I) w = 0. The normalized weights are called Distributive Mode in AHP, which shows the importance or priorities that should be distributed among the criteria and is given by the equation:

$$w_i = c_{ij} / \Sigma\, c_{kj} \qquad \text{(for any j).}$$

The principle of logical consistency is based on the belief that humans are capable of making coherent judgment when setting a logical hierarchy and priorities among the various parts of the issue. However, in real life, a person's preference may change due to certain circumstances or environment. To ensure a certain degree of consistency so that a reasonably sound and reliable result is obtained, the AHP measures the overall consistency using a term known as the consistency ratio. Saaty recommended the value of the consistency ratio to be 10% or less.

The generic AHP process can be summarized into the following steps:

1. Identify the problems to resolve
2. Develop a hierarchy of the problems in terms of the overall goal, attributes, decision criteria, and alternatives
3. Perform pair wise comparison at each level to establish relationships between multiple criteria
4. Perform consistency check at each level immediately after the pair-wise comparisons
5. Calculate the final weight ranking of the various alternatives
6. Synthesize the results and repeat as necessary

7.2.2 Research Methodology

The methodology adopted to develop the AHP was based on the list of Critical Operational Issues (COI). This process was iterative since the COIs were constantly revised as new scenarios were developed. The AHP was finalized after the mission scenarios and COIs were completed. Next, a questionnaire was developed and an internal survey was conducted among the team members and faculty advisors to gather suggestions for improvements to the questionnaire.

The target audiences for the survey were SMEs, namely academics, war fighters, technical specialists, and logistics officers. The computed weights of the AHP were subsequently used to evaluate three alternatives systems: EC2, System Y, and R2C2. This evaluation and analysis of alternatives represents an academic demonstration of the multicriteria decision-making process and the possible insights that could be gained from this approach.

7.2.3 Identifying the Issues

In order to develop a meaningful AHP, identifying critical criteria to measure the value or relative important aspects of the system was required. To accommodate such needs, development of the AHP started with identifying the COIs of the R2C2 system. COIs were identified by tracing back to the five scenarios explored in Chapter 2.0, discussing the system with the intended users, and examining all system requirements. A

total of nine COIs were developed and all represent critical functions of the R2C2 system. The COIs were then broken down into Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs), which are measures that express the extent to which a system accomplishes or supports a mission or task. They were designed to address the capabilities and suitability of the system. These two measures were further broken down into Measures of Performance (MOPs), which is a quantitative or qualitative measure of a system's capabilities or specific performance function. The following is the breakdown of the COIs, MOEs, MOSs, and MOPs:

1. COI – Is the R2C2 system able to provide sufficient communication capability for RCC?
    - 1.1 MOE – Satellite link capability
        - 1.1.1 MOP – Average signal range
        - 1.1.2 MOP – Call completion rate
        - 1.1.3 MOP – Average file transfer time over a network
        - 1.1.4 MOP – Proportion of communications link capacity utilized
    - 1.2 MOE – Organic sensors link capability
        - 1.2.1 MOP – Average signal range
        - 1.2.2 MOP – Call completion rate
        - 1.2.3 MOP – Average file transfer time over a network
        - 1.2.4 MOP – Proportion of communications link capacity utilized
    - 1.3 MOE – Network planning and control
        - 1.3.1 MOP – Average time to establish communications
        - 1.3.2 MOP – Average time to acquire terminals
    - 1.4 MOE – Receiving capability
        - 1.4.1 MOP – Message Completion Rate (MCR)
        - 1.4.2 MOP – Proportion of received reports acknowledged
        - 1.4.3 MOP – Proportion of uninterrupted communications
        - 1.4.4 MOP – Message accuracy
        - 1.4.5 MOP – Average time to acknowledge report
    - 1.5 MOE – Transmission capability
        - 1.5.1 MOP – Proportion of files transferred over a network
        - 1.5.2 MOP – Average data Message Completion Time (MCT)
        - 1.5.3 MOP – Average transmission backlog
        - 1.5.4 MOP – Average duration of transmission wait
        - 1.5.5 MOP – Proportion of retransmitted messages

2. COI – Is the deployability of the R2C2 system satisfactory for the mission accomplishment?
    - 2.1 MOE – Physical robustness
        - 2.1.1 MOP – Maximum height of a drop that the R2C2 system can withstand without functional failure
        - 2.1.2 MOP – Intensity of vibration that the R2C2 system can withstand without functional failure

2.1.3 MOP – Duration of vibration that the R2C2 system can withstand without functional failure
2.1.4 MOP – Mean time to critical failure in sandy environment
2.1.5 MOP – Mean time to critical failure in humid environment

2.2 MOE – Responsiveness
2.2.1 MOP – Mean time to marshal the R2C2 system
2.2.2 MOP – Mean time to set up the R2C2 system at the operating site
2.2.3 MOP – Mean time to breakdown the R2C2 system

2.3 MOE – Transportability
2.3.1 MOP – Dimension of the R2C2 system
2.3.2 MOP – Weight of the R2C2 system (per case)
2.3.3 MOP – Number of modules

3. COI – Is the R2C2 system interoperable with other legacy systems and with the communications systems of other friendly forces and the host country?

3.1 MOE – Communication capability with inorganic sensors
3.1.1 MOP – Duration of connection without interruption
3.1.2 MOP – Average time to establish connection
3.1.3 MOP – Average data exchange time
3.1.4 MOP – Proportion of successful data exchanges
3.1.5 MOP – Reasons for failure to exchange data
3.1.6 MOP – Proportion of data files useable without modification (i.e., the ratio of the total number of data files useable without modification to the total number of data files received)

3.2 MOE – Communication capability with other R2C2 systems
3.2.1 MOP – Duration of connection without interruption
3.2.2 MOP - Average time to establish connection
3.2.3 MOP – Average data exchanged time
3.2.4 MOP – Proportion of successful data exchanges
3.2.5 MOP – Reasons for failure to exchange data
3.2.6 MOP – Proportion of data files useable without modification (i.e., the ratio of the total number of data files useable without modification to the total number of data files received)

3.3 MOE – Reach back capability RCCs
3.3.1 MOP – Duration of connection without interruption
3.3.2 MOP – Average time to establish connection
3.3.3 MOP – Average data exchange time
3.3.4 MOP – Proportion of successful data exchanges
3.3.5 MOP – Reasons for failure to exchange data
3.3.6 MOP – Proportion of data files useable without modification (i.e., the ratio of the total number of data files useable without modification to the total number of data files received)

3.4 MOE – Communication capability with coalition partners
3.4.1 MOP – Duration of connection without interruption
3.4.2 MOP – Average time to establish connection
3.4.3 MOP – Average data exchange time
3.4.4 MOP – Proportion of successful data exchanges

3.4.5 MOP – Reasons for failure to exchange data
3.4.6 MOP – Proportion of data files useable without modification (i.e., the ratio of the total number of data files useable without modification to the total number of data files received)

3.5 MOE – Communication capability with civilian organizations
3.5.1 MOP – Duration of connection without interruption
3.5.2 MOP - Average time to establish connection
3.5.3 MOP – Average data exchange time
3.5.4 MOP – Proportion of successful data exchanges
3.5.5 MOP – Reasons for failure to exchange data
3.5.6 MOP – Proportion of data files useable without modification (i.e., the ratio of the total number of data files useable without modification to the total number of data files received)

3.6 MOE – GIG access capability
3.6.1 MOP – Duration of connection with NIPRNet and SIPRNet simultaneously without interruption
3.6.2 MOP – Duration of connection with NIPRNet and CENTRIXS simultaneously without interruption
3.6.3 MOP – Duration of connection with SIPRNet and CENTRIXS simultaneously without interruption

4. COI – Is the R2C2 system able to provide situational assessment to RCCs?
4.1 MOE – Organic sensors to the R2C2 system operator
4.1.1 MOP – Footprint (diameter) of supporting area
4.1.2 MOP – Frequency of information update

4.2 MOE – Inorganic sensors to the R2C2 system operator
4.2.1 MOP – Footprint (diameter) of supporting area
4.2.2 MOP – Frequency of information update

4.3 MOE – R2C2 to RCC
4.3.1 MOP – Average time to filter data after collection
4.3.2 MOP – Average time to compile data after collection
4.3.3 MOP – Frequency of information update

5. COI – Does the R2C2 system provide a sufficient level of information security for successful mission accomplishment?
5.1 MOE – Data security
5.1.1 MOP – Proportion of completed unauthorized file accesses (i.e., the ratio of the total number of completed unauthorized file accesses to the total number of attempted unauthorized file accesses)
5.1.2 MOP – Proportion of correct security classifications (i.e., the ratio of the total number of files/documents properly marked by the system to the total number of files/documents generated)
5.1.3 MOP – Average adequacy ratings of access control procedures

(i.e., the average ratings of the adequacy of control procedures or processes to prevent unauthorized access to a system)

5.1.4 MOP – Average adequacy ratings of controls to confirm user access (i.e., the average ratings of the adequacy of controls to confirm user access to authorized information in a system)

5.2 MOE – Network security

5.2.1 MOP – Proportion of completed unauthorized network accesses (i.e., the ratio of the total number of completed unauthorized network accesses to the total number of attempted unauthorized network accesses)

5.2.2 MOP – Average adequacy ratings of procedures for networks and communications security (i.e., the average ratings of the procedures or processes to provide for networks and communications security of a system)

5.2.3 MOP – Proportion of completed unauthorized logons (i.e., the ratio of the total number of completed unauthorized logons to the total number of attempted unauthorized logons)

5.3 MOE – Physical security

5.3.1 MOP – Average adequacy ratings of physical security (i.e., the average ratings of the adequacy of physical security of a system. Individual ratings can range from 1 (completely disagree that security is adequate) to 9 (completely agree that security is adequate)

5.3.2 MOP –Average adequacy ratings of plans, training, and personnel procedures for security: The average ratings of adequacy of the unit's Standard Operating Procedure (SOP), personnel security, training, and the Program Manager's security plan for a system.

6. COI – Is the R2C2 system flexible enough to support various types of mission?

6.1 MOE – Modularity

6.1.1 MOP – Number of different types of missions that the R2C2 system can support

6.2 MOE – Scalability

6.2.1 MOP – Maximum number of operators that the R2C2 system can support

6.2.2 MOP – Maximum area of operation that the R2C2 system can support

6.3 MOE – Sustainability

6.3.1 MOP – Number of operators/scouts

6.3.2 MOP – Total R2C2 system operating hours (restricted by power capacity)

6.3.3 MOP – Level of logistic support for the R2C2 system crew

7. COI – Does the R2C2 system meet the reliability needs for successful mission accomplishment?
    - 7.1 MOS – Mission success
        - 7.1.1 MOP- Satellite link-up availability
        - 7.1.2 MOP –Number of spare parts
        - 7.1.3 MOP – Maximum hours of generator run time
        - 7.1.4 MOP – Availability of other supporting infrastructure
    - 7.2 MOS – High quality components
        - 7.2.1 MOP – Mean Time Before Critical Failure (Critical Failure = Main Operating Laptop failure)
        - 7.2.2 MOP – Mean Time Before Major Failure (Major Failure = Organic sensor failure)
        - 7.2.3 MOP – Mean Time To Repair

8. COI – Is the R2C2 system easily maintained by its intended users?
    - 8.1 MOS – Built in test (BIT)
        - 8.1.1 MOP –Proportion of diagnosable failures (i.e., the ratio of the total number of possible system failures to the total number of diagnosable failures)
    - 8.2 MOS – Ease of repair
        - 8.2.1 MOP – Mean time required to repair
        - 8.2.2 MOP – Tools needed for repair
    - 8.3 MOS – Availability of repair parts
        - 8.3.1 MOP – Proportion of the R2C2 system component that is commercially available

9. COI – Are the R2C2 team members able to fully utilize the capability of the R2C2 system?
    - 9.1 MOS – Ease of operation
        - 9.1.1 MOP – The proportion of R2C2 system critical tasks attempted (i.e., the ratio of the total number of system critical tasks attempted by the test players to the total number of tasks presented)
        - 9.1.2 MOP – The proportion of R2C2 system critical tasks finished (i.e., the ratio of the total number of system critical tasks the test player believe they have finished to the total number of tasks attempted)
        - 9.1.3 MOP – The average usability ratings of R2C2 system critical tasks (i.e., the average ratings of system critical task characteristics given by test players at the end of each task trial, based on the ease-of-use or task difficulty)
        - 9.1.4 MOP – The average time required to successfully complete system critical tasks (excluding timeouts for breaks or interruptions)
        - 9.1.5 MOP – The reasons that R2C2 system critical tasks were not completed (i.e., insufficient manpower, poor display, poor control arrangement, or poor training)

7.2.4 Developing Hierarchy

Previously identified COIs, MOEs, MOSs, and MOPs served two purposes. First, they provided a starting point of developing the Test and Evaluation Master Plan (TEMP) of the R2C2 system in the near future. The second purpose, and the one chosen for our use, was to provide a baseline to generate the hierarchy of comparison criteria for the AHP. Each COI, MOE, MOS, and MOP was reviewed and transformed into the comparable criteria. Some of them were implemented directly as one of the comparison criteria and some of them were implied.

As shown in Figure 40, this model was comprised of three levels of criteria. The first-level criteria were Operations Capabilities, Technical Performance, and Integrated Logistics Support (ILS).

The second-level criteria were developed for each criterion defined at the first level. For Operations Capabilities, the criteria were Interoperability, Flexibility, Ease of Operations, Information Security, Deployability, and Situation Assessment. For Technical Performance, the criteria were Local Communications and Long Haul Communications. For ILS, the criteria were Reliability, Maintainability, Spares Support, Training, and Support Test Equipment.

Finally, the third-level criteria were developed where necessary. For Interoperability, the criteria were Civilian Networks, Coalition Network, and GIG Access. For Flexibility, the criteria were Modularity, Scalability, and Sustainability. For Ease of Operations, the criteria were Standardized Controls and Layout and Visual. For Information Security, the criteria were Network Security, Data Security, and Physical Security. For Deployability, the criteria were Weight, Physical Dimension, Setup Time, and Extraction Time. For Situation Assessment, the criteria were Organic Sensor footprint of supporting area, Organic Sensor refresh rate, Inorganic Sensor footprint of supporting area, and Inorganic Sensor refresh rate.

Under Technical Performance, the third-level criteria for Local and Long Haul Communications were Bandwidth, Range, Refresh Rate, Storage Capacity, Power, Link Reliability, and Link Availability. For ILS, the third-level criteria were defined only for Maintainability; they were Self Test and Ease of Repair.

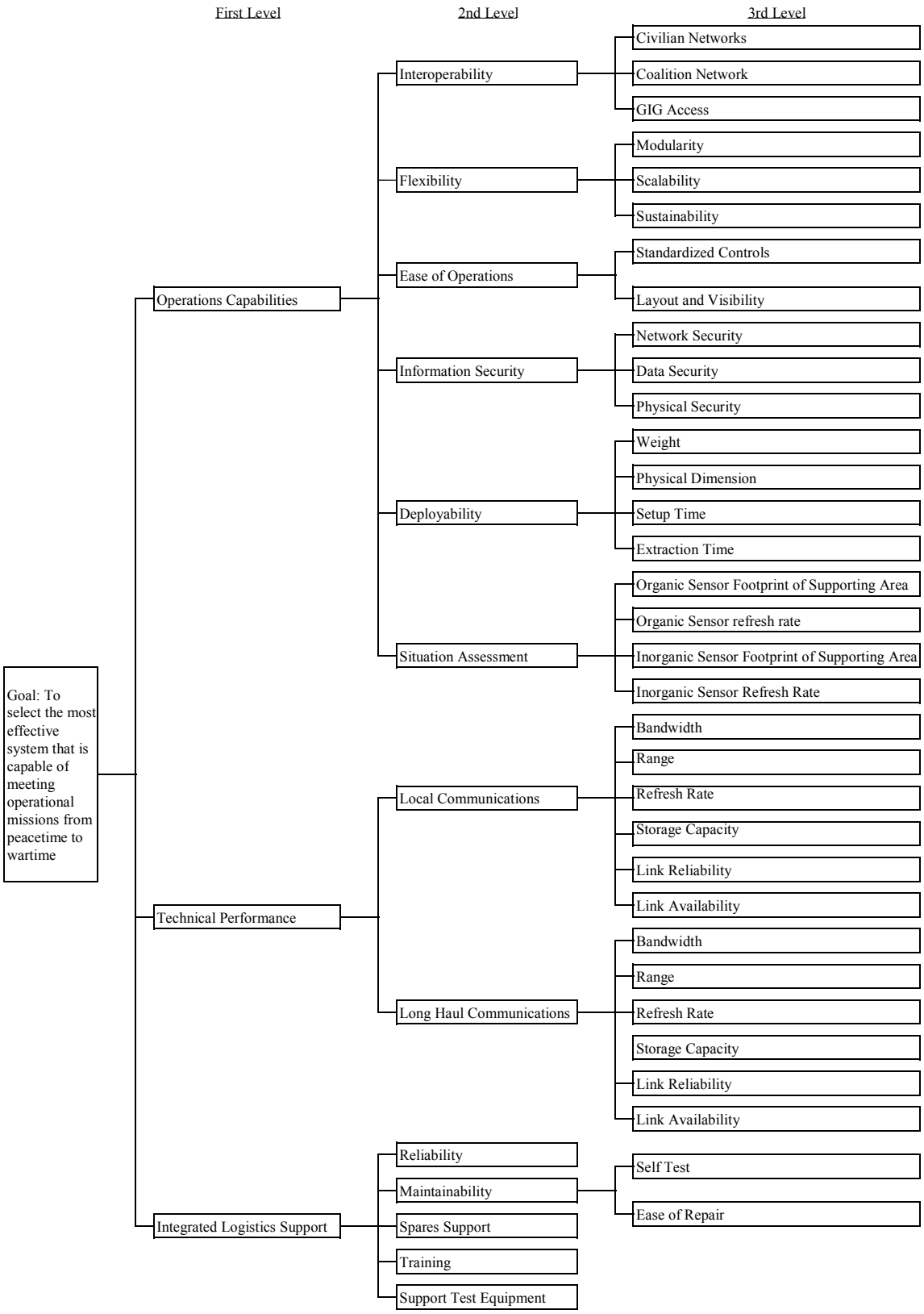


Figure 40: An Overview of R2C2 Analytic Hierarchy Process

7.2.5 AHP Results and Analysis

In this section, we present the results of the AHP process, using the AHP-based software, Expert Choice, to develop the multicriteria decision-making process and arrive at our conclusions. Given that a sample size of 30 were required to achieve a statistical significance, a total of 30 surveys were received with the participant profile as shown in Figure 41.

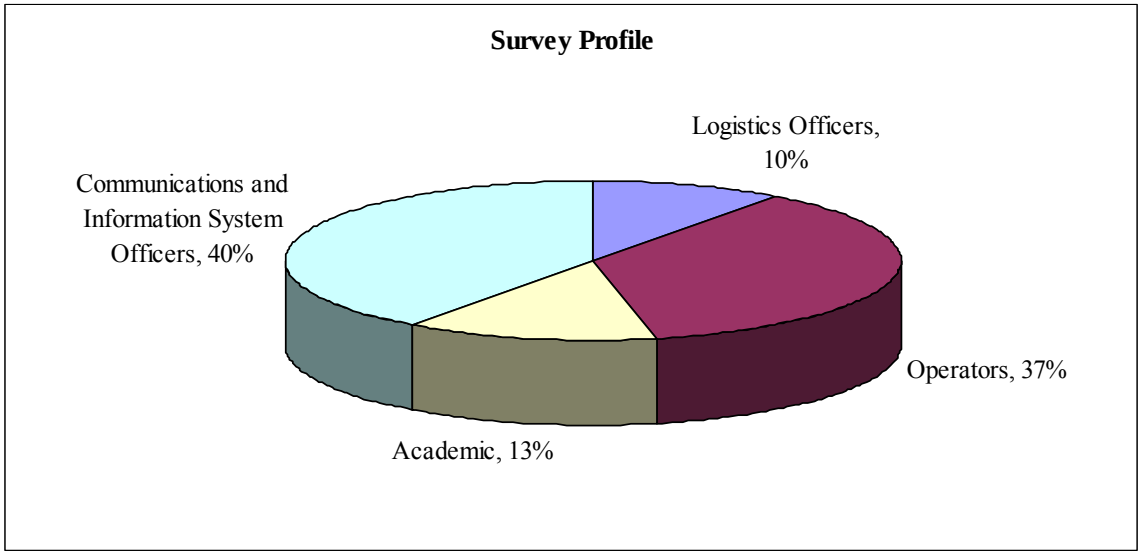


Figure 41: Survey Participant Profile

The raw data was first analyzed using Minitab software to determine whether there was any statistical difference between the inputs from the four groups of participants. It was assumed that the 30 samples were independent and identically distributed. However, with a small sample size for each group, normality could not be assumed. Hence, the nonparametric Kruskal-Wallis one-way analysis of variance by rank was used for the analysis.[116] The null hypothesis was that there were no differences in the pair-wise judgment between groups. P-values less than 0.1 were an indication that at least one of four groups' weighting was different from the other three.

Data scaling was performed on the raw data by subtracting 1 if the criterion C_i was more important than criterion C_i, and adding 1 if criterion C_j was more important

[116] Condon et al., "Visualizing Group Decisions in the Analytic Hierarchy Process Models," *Computers and Operations Research*, 2003, pp. 60-63.

than criterion C_i. With this modification, the scale for each pair-wise comparison ranged from −8 to 8. The results of the Kruskal-Wallis one-way analysis for the first- and second-level pair-wise comparison judgment between the various groups was tabulated in Table 19. The results showed that statistically there were no significant differences ($p \geq 0.1$) for the pair-wise judgment between the groups. However, it was observed that the Kruskal-Wallis test on Interoperability versus Information Security comparison yielded a p-value of 0.1, which is a borderline situation.

Description of Pair-Wise Comparison	**p-value**
First-Level Hierarchy	
Operations Capabilities vs. Technical Performance	0.871
Operations Capabilities vs. ILS	0.896
Technical Performance vs. ILS	0.184
Second-Level Hierarchy – Operations Capabilities	
Interoperability vs. Flexibility	0.175
Interoperability vs. Ease of Operations	0.578
Interoperability vs. Information Security	0.100
Interoperability vs. Deployability	0.303
Interoperability vs. Situation Assessment	0.657
Flexibility vs. Ease of Operations	0.968
Flexibility vs. Information Security	0.420
Flexibility vs. Deployability	0.732
Flexibility vs. Situation Assessment	0.626
Ease of Operations vs. Information Security	0.696
Ease of Operations vs. Deployability	0.959
Ease of Operations vs. Situation Assessment	0.582
Information Security vs. Deployability	0.772
Information Security vs. Situation Assessment	0.626
Deployability vs. Situation Assessment	0.778
Second-Level Hierarchy – Technical Performance	
Local Communications vs. Long Haul Communications	0.908
Second-Level Hierarchy – ILS	
Reliability vs. Maintainability	0.515
Reliability vs. Spares Support	0.551
Reliability vs. Training Requirements	0.261
Reliability vs. Support Test Equipment	0.533
Maintainability vs. Spares Support	0.271
Maintainability vs. Training Requirements	0.113
Maintainability vs. Support Test Equipment	0.145
Spares Support vs. Training Requirements	0.291
Spares Support vs. Support Test Equipment	0.670
Training Requirements vs. Support Test Equipment	0.645

Table 19: Results of the Kruskal-Wallis One-Way Analysis

The Kruskal-Wallis one-way analysis concluded that the AHP could be further analyzed considering the 30 survey samples as a homogenous group. There are two approaches to compute the combined weights for the hierarchy: weighted arithmetic mean or geometric mean of the individual judgments.[117] If weight p^k is assigned to decision maker k, then the weighted arithmetic mean is given by

$$c_{ij} = p^1 c_{ij}^{\ 1} + p^2 c_{ij}^{\ 2} + \ldots + p^n c_{ij}^{\ n}.$$

Using the geometric mean approach, the individual judgments of the n participants are combined to produce

$$c_{ij} = [\ c_{ij}^{\ 1} \text{ x } c_{ij}^{\ 2} \text{ x } \ldots \text{ x } c_{ij}^{\ n}]^{\ 1/n}.$$

The geometric mean was adopted for the analysis as it preserved the reciprocal property when each participant was assigned equal weight.[118] The geometric mean was also found to be the most common approach used by groups to set priorities.[119] Using this approach, the geometric mean of the 30 survey samples for each pair-wise comparison in the R2C2 AHP was computed and input into the Expert Choice software.

Figure 42 shows the weights of the first-level comparison criteria. As can be seen, the computation of the survey resulted in the weights attained in Operation Capability (0.481), Technical Performance (0.348), and ILS (0.171) in order of highest to least importance.

---

[117] Bolloju, N., "Aggregation of Analytic Hierarchy Process Models Based on Similarities in Decision Makers' Preference," *European Journal of Operational Research*, 2001, pp. 12-15.

[118] Aczel et al., "Procedures for Synthesizing Ratio Judgments," *Journal of Mathematical Psychology*, 1983, pp. 4-10.

[119] Condon et al., "Visualizing Group Decisions in the Analytic Hierarchy Process Models," *Computers and Operations Research*, 2003, pp. 60-68.

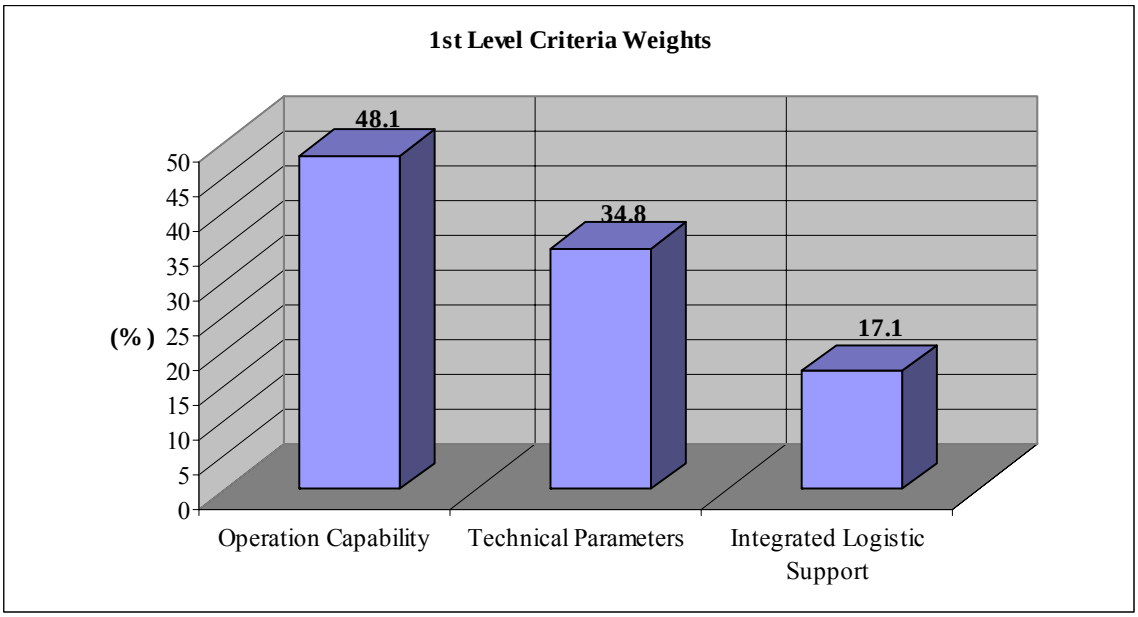


Figure 42: First-Level Criteria Weights

Similarly, pair-wise comparison results from the survey were computed and weights for the second-level criteria were attained. The results are shown in Figures 43, 44, and 45:

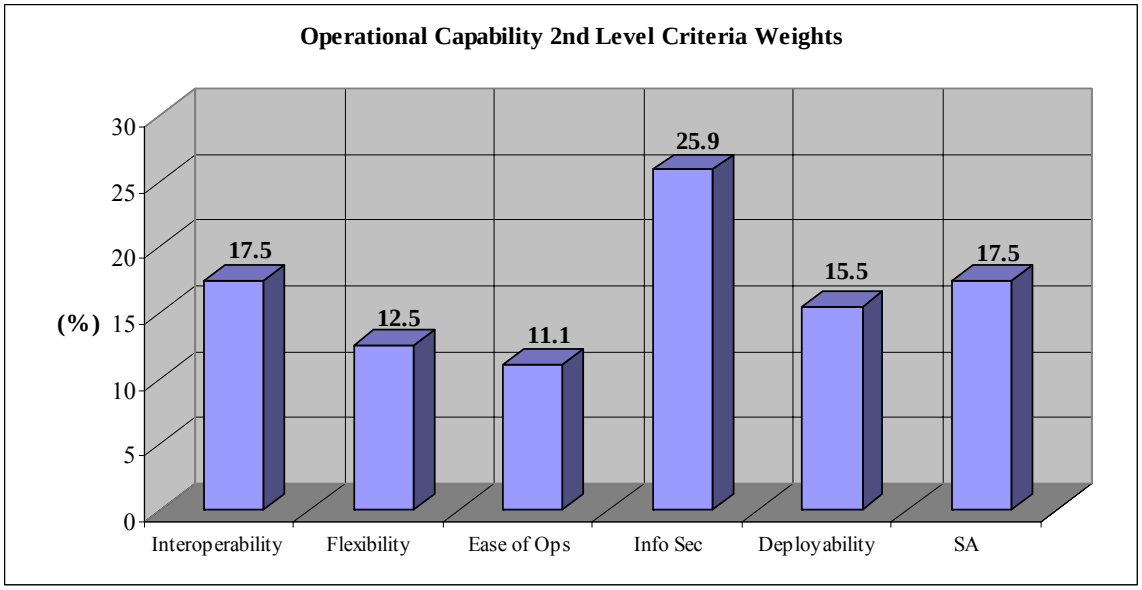


Figure 43: Second-Level Weights – Operations Capability

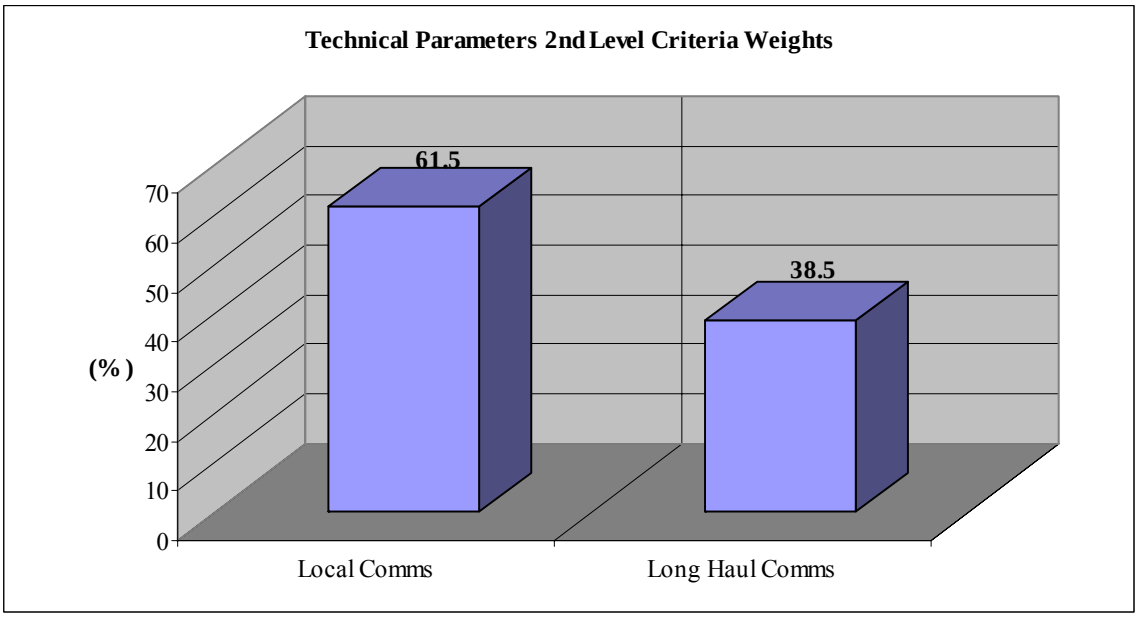


Figure 44: Second-Level Weights – Technical Parameters

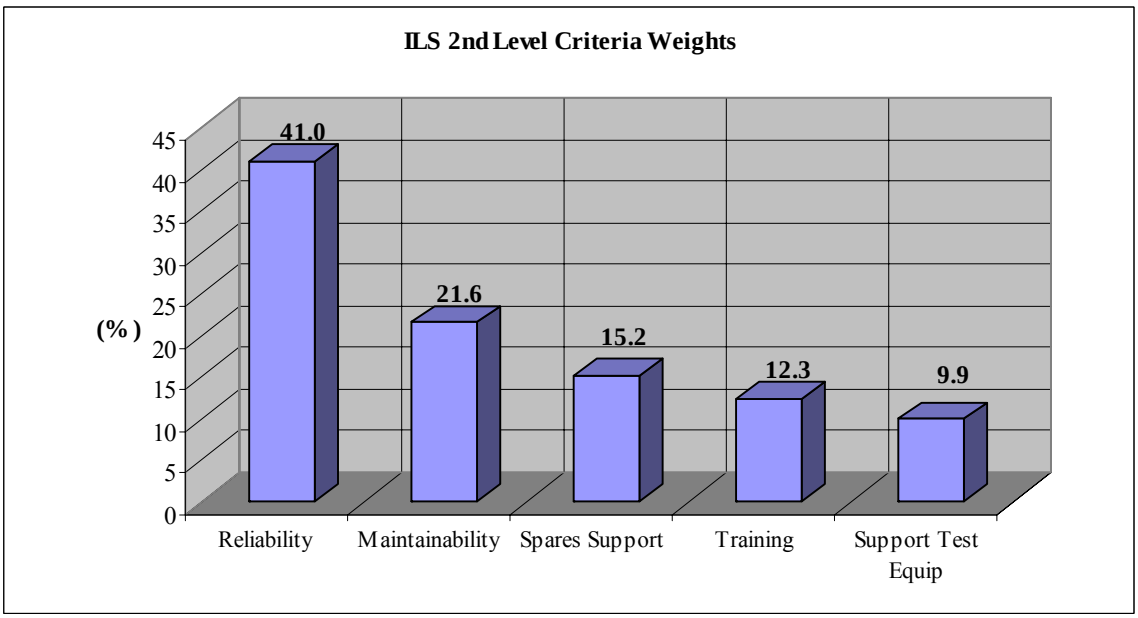


Figure 45: Second-Level Weights – ILS

Lastly, results of the third-level comparison criteria under each second-level criterion were computed from the survey results and compiled in Table 20, with their respective weights in parentheses:

Second-Level Criteria	Third-Level Criteria
Interoperability (0.084)	Civilian Networks (0.019)
	Coalition Networks (0.028)
	GIG Access (0.037)
Flexibility (0.060)	Modularity (0.016)
	Scalability (0.017)
	Sustainability (0.027)
Ease of Operations (0.053)	Standardized Controls (0.023)
	Layout and Visibility (0.03)
Information Security (0.125)	Network Security (0.053)
	Data Security (0.042)
	Physical Security (0.03)
Deployability (0.075)	Weight (0.014)
	Physical Dimensions (0.018)
	Setup Time (0.026)
	Extraction Time (0.018)
Situational Assessment (0.084)	Organic Sensor Footprint (0.028)
	Organic Sensor Refresh Rate (0.022)
	Inorganic Sensor Footprint (0.019)
	Inorganic Sensor Refresh Rate (0.016)
Local Communication (0.214)	Bandwidth (0.035)
	Range (0.031)
	Refresh rate (0.023)
	Storage capacity (0.018)
	Link Reliability (0.059)
	Link Availability (0.047)
Long Haul Communication (0.134)	Bandwidth (0.023)
	Range (0.022)
	Refresh Rate (0.013)
	Storage Capacity (0.011)
	Link Reliability (0.035)
	Link Availability (0.029)
Maintainability (0.037)	Self Test (0.012)
	Ease of Repair (0.025)

Table 20: Third-Level Criteria

To check for inconsistency in the ranking process, each stage of the hierarchy was subjected to the consistency check. Figure 46 is a screenshot of the Expert Choice program displaying the consistency index of 0.01 for the second-level criteria of operation capability. According to Saaty, acceptable inconsistency index should be below 0.1. None of the ranks in our AHP exceeded the inconsistency index of 0.1.

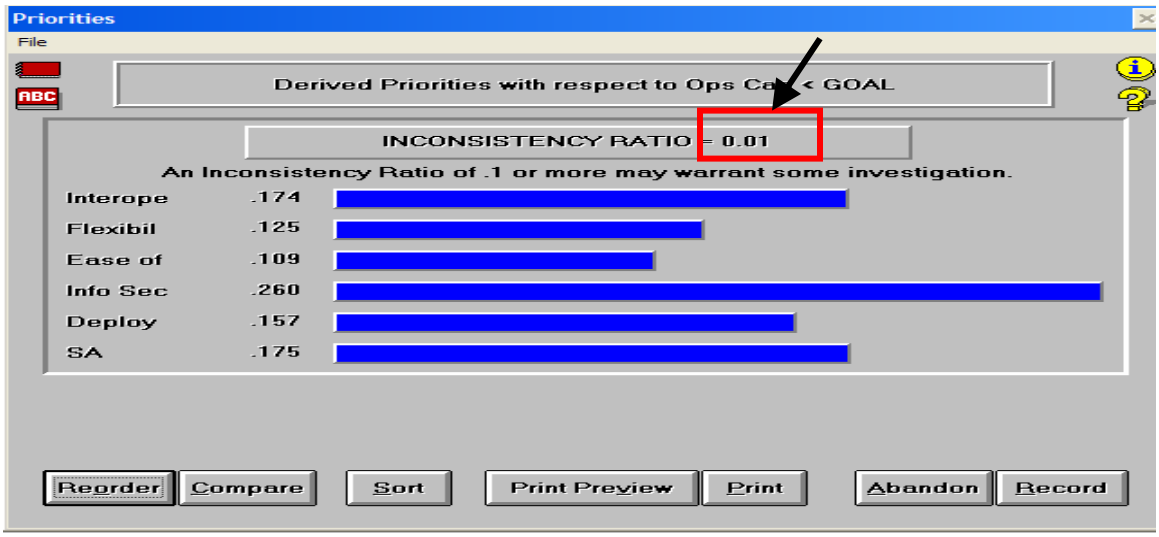


Figure 46: Screenshot of Expert Choice – Inconsistency Index

7.2.6 Comparisons of Three Systems

These weightings, developed from inputs from the survey, formed the basis for the evaluation of the three systems: JSIC EC2, System Y, and R2C2. The EC2 was developed in 2003 by JSIC to provide RCCs and JTF commanders the capability to host services on classified and unclassified networks when they were away from headquarters to maintain situation assessment.[120] The package consists of laptops, routers, and other pieces of equipment that can be easily packed in a hard case and rolled into a car, airplane, helicopter, or "humvee."[121] System Y is a proposed proprietary system under

[120] Sgt. John Cupp, USA, USJFCOM Public Affairs, "Ainsworth Honored as Command's Joint Junior Officer of the Quarter," 2 March 2006, http://www.jfcom.mil/newslink/storyarchive/2006/pa030206.htm. Last accessed in May 2006.

[121] Sgt. John Cupp, USA, USJFCOM Public Affairs, "New Suffolk Facility to Provide Warfighter Rapid Solutions," 10 September 2004, http://www.jfcom.mil/newslink/storyarchive/2004/pa091004.htm. Last accessed in May 2006.

the contract of RRK, therefore the name of the company and the detailed information of the system will remain anonymous.

The problem statement of the project was to examine the possibility of a rapidly deployable, C2 system that met the needs of RCCs in providing situational and communication capabilities through the range of military operations. Such a system would maximize the use of existing military systems, COTS systems, and coalition systems. The end objective was to develop a standardized, integrated, modular and scaleable Joint Command, Control, and Collaboration system. The system would have a small footprint to be utilized by first responders that were both interoperable and flexible.

In particular, the BAA had directed for a standalone, lightweight system capable of being transported by one or two persons as checked luggage on commercial or military transport aircraft. The desired functional capabilities were:

- Provide capability to connect to two GIG-accessible, crypto-covered networks at once (e.g., NIRPRNET, SIPRNET, CENTRIXS)
- Provide secure wireless to clients
- Utilize Everything over Internet Protocol (EoIP)
- Provide Net Centric operations to the maximum extent possible
- Demonstrate multimode (data, video, and voice) operations
- Provide a minimum of four Voice over IP (VoIP) telephonic instruments
- Must be able to use thin or thick clients, and must support five clients (threshold)/15 clients
- Provide radio with 1.024 Mbps threshold; 4.196 Mbps objective per network
- Provide reliability, maintainability, availability, built-in test and logistic support as an objective

7.2.6.1 Assessment on Operational Capabilities

In terms of operational capabilities, all three systems were rated as equal with regard to civilian networks. The reason being that as COTS systems, they would have equal access to the Internet and hence, no particular system would have an advantage over the other with regard to this criterion.

The same could not be said for other forms of networks such as the coalition networks and having GIG access. Both System Y and R2C2 had direct access to CENTRIX and SIPRNET, hence they had greater interoperability as compared to EC2.

By virtue of its lightweight nature, its less complex architecture, and having fewer components, EC2 was assessed to fare better than its counterparts in the areas of weight, dimension, ease of transportability, and setup and extraction time. In contrast, R2C2 had the lowest score in these criteria, as it was designed with a Local Communications Suite and portable power generator for greater mission capability and sustainability. Table 21 is a summary of the considerations used in the evaluation of the three systems:

Subcriteria	Assessment
Civilian Networks	All had equal capability that allowed access to Internet.
Coalition	System Y and R2C2 were ranked better than EC2 because they had access to CENTRIX, the coalition network.
GIG Access	System Y and R2C2 fared better than EC2 because EC2 does not have SIPRNET access.
Modularity	All three systems were modular in design.
Scalability	Modular design allowed hardware scalability. System Y fared better because it allowed three simultaneous networks access, which meant more people could connect up at any one time. R2C2 with two simultaneous networks was ranked second, followed by EC2.
Sustainability	R2C2 was better than System Y and EC2 because R2C2 was equipped with portable generator power.
Standardized Controls	All systems were on equal footing because they used COTS technology which was driven by industry standards.
Layout and Visibility	All systems were ranked equally because they used COTS technology, driven by industry standards.
Network Security	All systems were ranked equally because they provided VPN tunnel and NSA type 1 security features.
Data Security	System Y and R2C2 had data encryption; hence they were ranked better than EC2.
Physical Security	All three systems were designed to have checkable cases and carry on cases, hence the level of physical security were comparable.
Weight and Dimension	EC2 was ranked the best, followed by System Y. R2C2 fared the worst because of additional cases for generator and local communication suite for added capability.
Setup Time	EC2 was likely to be faster with a simple architecture while System Y and R2C2 were comparable.
Extraction Time	EC2 was likely to be faster with a simple architecture while System Y and R2C2 were comparable.
Organic Sensor Footprint	R2C2 had a Local Communication Suite compared to EC2 and System Y, hence a larger footprint for the supporting area.
Organic Sensor Refresh Rate	With a Local Communication Suite, situation assessment update for R2C2 was faster than System Y and EC2.
Inorganic Sensor Footprint	All three systems had not designed for this feature, so they were given equal preferences.
Inorganic Sensor Refresh Rate	All three systems had not designed for this feature, so they were given equal preferences.

Table 21: Operational Capability Considerations

7.2.6.2 Assessment on Technical Performance

Since both EC2 and System Y have no local communications capability, the preference was given to R2C2. Further considerations for the evaluation of third-level criteria for Long Haul Communications were summarized in Table 22.

Sub-criteria	Assessment
Bandwidth	System Y and R2C2 used the same satellite system (Swedish) which was more capable than INMARSAT, i.e., 4 Mbps duplex versus 128 Kbs.
Range	All systems were ranked equally as satellite communication coverage were similar.
Storage Capacity	All systems were rank equally as similar COTS technologies were used.
Refresh Rate, Link Reliability, and Link Availability	The three systems were comparable in performance because they were GEO stationary satellites and the mode of operations was primarily stationary.

Table 22: Technical Performance Considerations

7.2.6.3 Assessment on ILS

This was one area where the system with the simplest architecture fared better. The three systems were generally assessed to be comparable given the fact that they have been built on tried and trusted COTS technology. However, given the more austere operating conditions, it was assumed that the system with the smallest logistic footprint would fare better than one that continually relied on logistic support to sustain its operations. In this respect, EC2, with a simpler setup and less complex equipment and architecture, would fulfill its mission with fewer reliability issues. With fewer components and a simpler architecture, the overall reliability of such a system would be higher than a complex system with many components, each imposing a logistic and reliability strain on the overall system performance. This same reasoning was applied to the training aspect, where a system with fewer components would be easier to train personnel as compared to a system with greater capability and complexity. A summary of the ILS considerations are annotated in Table 23.

Subcriteria	Assessment
Reliability	System Y and R2C2 used similar COTS technologies and the similar GEO satellite systems; hence, they were assessed to give comparable reliability figures. However, the reliability of EC2, with similar COTS technologies and fewer modules, was assessed to be slightly better.
Self Test	Due to the lack of information for assessment, the three systems were ranked equally.
Ease of Repair	Due to the lack of information for assessment, the three systems were ranked equally.
Spares Support	The number of spares to cater was assessed to be comparable for all three systems as they used similar COTS technologies. However, R2C2 with its power generator and local communication suite would mean slightly more spares support was required. EC2, having the fewest components, was ranked the best.
Training	Based on the number of modules in each system, training requirement was assessed to be more demanding for R2C2, followed by System Y and EC2. Hence, EC2 fared the best, followed by Sys Y and R2C2.
Support Test Equipment	Due to the lack of information for assessment, the three systems were ranked equally.

Table 23: ILS Considerations

7.2.6.4 Overall Synthesis

As shown in Figure 47, R2C2 was found to be the most suitable system with the highest weight of 0.427. R2C2 had a clear lead over the other two alternatives. Because System Y and EC2 weights were close with 0.29 and 0.284, respectively, it was necessary to carry out a sensitivity analysis of the alternatives, with respect to the criteria.

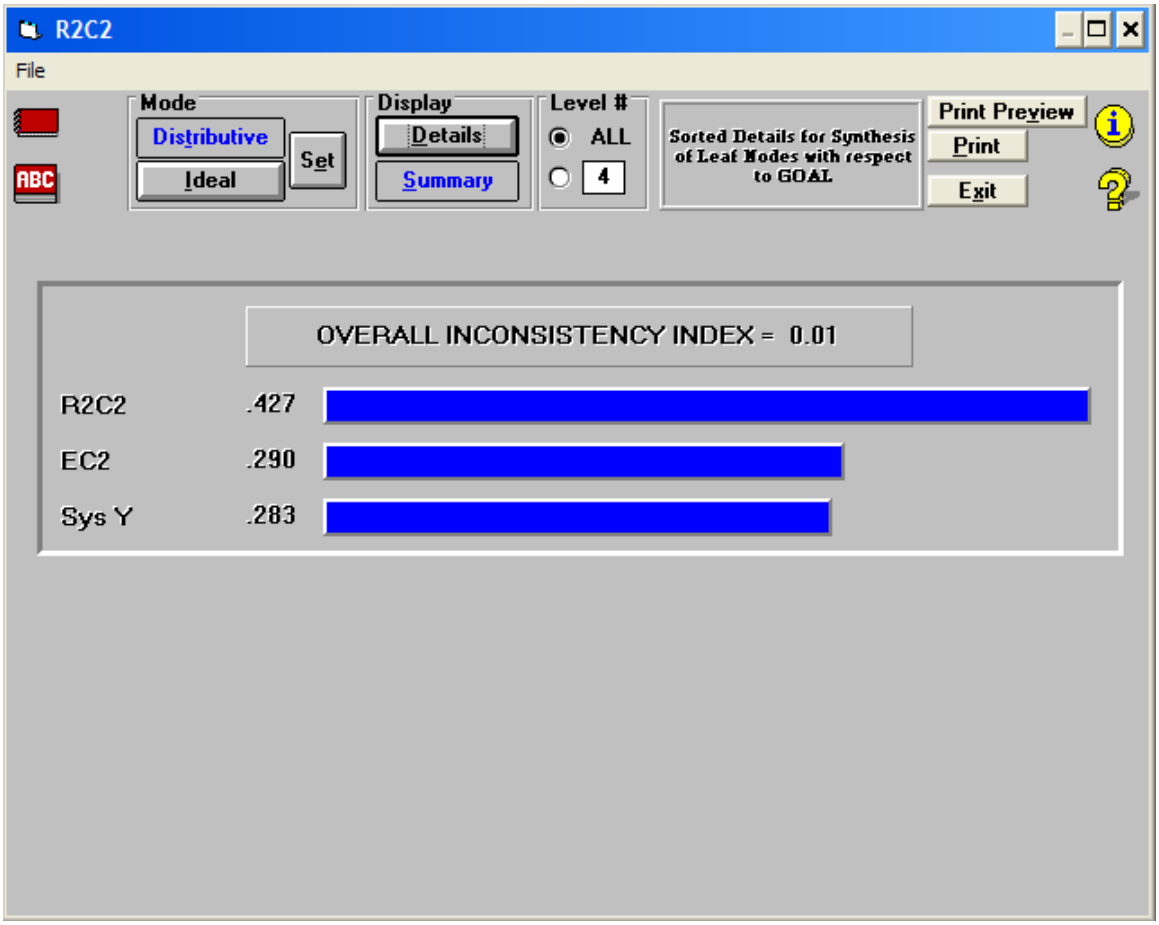


Figure 47: Overall Syntheses

7.2.7 Overall Sensitivity Analysis Graph

A sensitivity analysis of the alternatives, with respect to the criteria, was carried out. This would establish how sensitive the alternatives were to the criteria and provide additional insights into the model. In particular, we would focus on the criteria that would result in alternative reversals. Figure 48 shows the sensitivity analysis as a result of changing the Operational Capability weight. The original decision outcome is displayed in Figure 47 with the rankings being: R2C2 (0.427), EC2 (0.290), and

System Y (0.283). As a result of increasing the weight (from 48.1% to 57.5%) on Operational Capability, it was observed that R2C2 still managed to retain its top ranking. However, it was observed that EC2 replaced System Y as the second-ranked system.

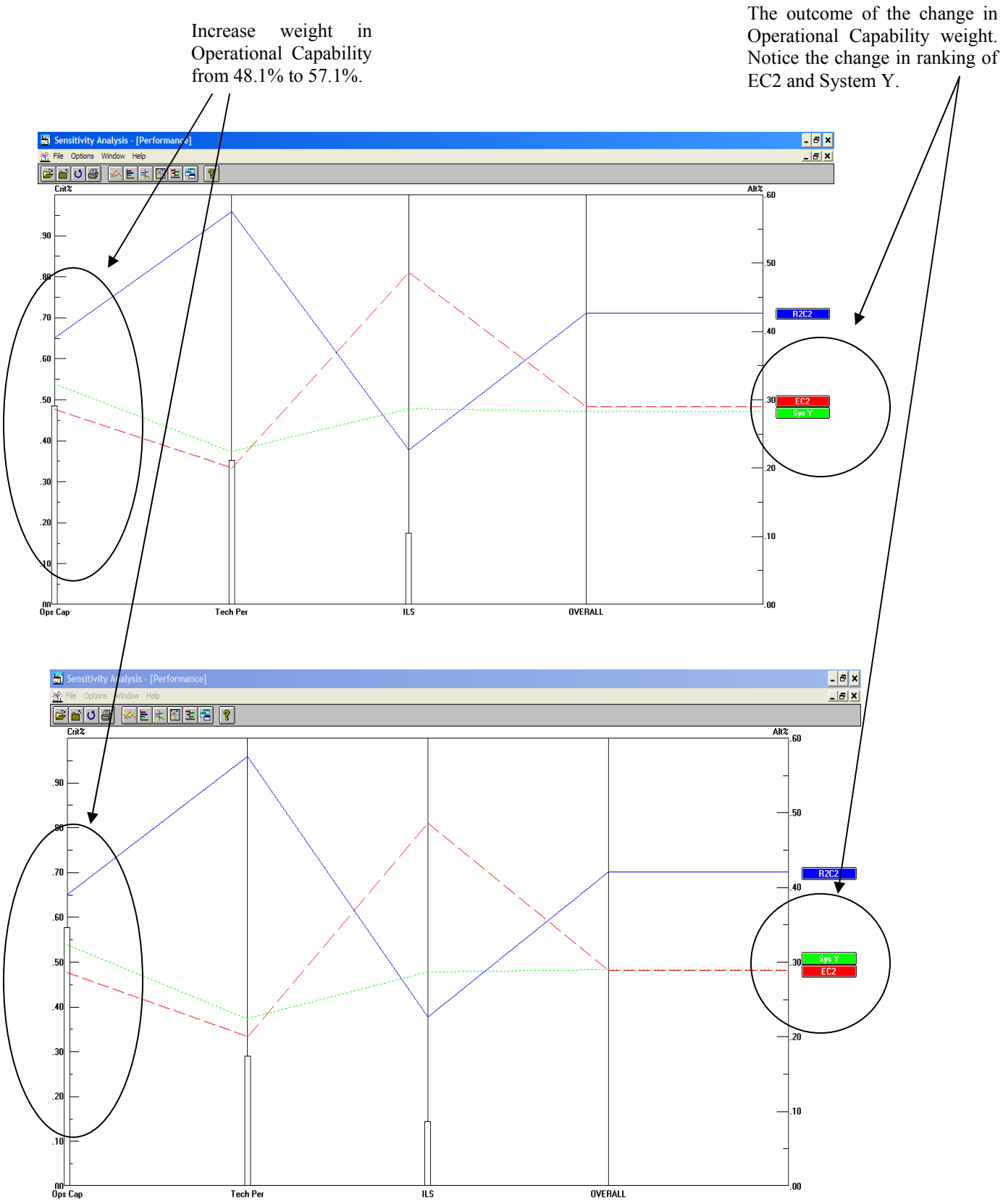


Figure 48: Sensitivity Analysis of Alternatives – Change in Operational Capability Weight

Likewise, the weight of Technical Performance and ILS were varied to assess if it resulted in a change of ranking or rank reversals of the original decision outcome. It was noted that variation of the three main criteria of Operational Capabilities, Technical Performance, and ILS did not result in rank reversal for R2C2. It remained the first choice among the three alternatives in all weights for the main criteria. However, for the other two alternatives of EC2 and System Y, the changes in weights did result in rank reversals. Tables 24, 25, and 26 show the amount of "perturbations" in Operations Capabilities, Technical Performance, and ILS, respectively, which resulted in alternative reversal.

Criteria	Original Weights	Weights Resulting in Alternative Reversal (Increasing Weights of Operations Capability)	Ranking (Original % in Parentheses)
Ops Capabilities	48.1%	57.5%	R2C2 – 42.1% (42.7%)
Technical Performance	34.8%	28.5%	EC2 – 28.9% (29.0%)
ILS	17.1%	14.0%	System Y – 29.0% (28.3%)

Table 24: Changes in Weights of Operational Capabilities Resulting in Alternative Reversal

Criteria	Original Weights	Weights Resulting in Alternative Reversal (Increasing Weights of Technical Performance)	Ranking (Original % in Parentheses)
Ops Capabilities	48.1%	36.6%	R2C2 – 46.3% (42.7%)
Technical Performance	34.8%	50.4%	EC2 – 26.8% (29.0%)
ILS	17.1%	13.0%	System Y – 26.9% (28.3%)

Table 25: Changes in Weights of Technical Performance Resulting in Alternative Reversal

Criteria	Original Weights	Weights Resulting in Alternative Reversal (Increasing Weights of ILS)	Ranking (Original % in Parentheses)
Ops Capabilities	48.1%	31.5%	R2C2 – 35.8% (42.7%)
Technical Performance	34.8%	22.8%	EC2 – 35.8% (29.0%)
ILS	17.1%	45.7%	System Y – 28.4% (28.3%)

Table 26: Changes in Weights of ILS Resulting in Alternative Reversal

R2C2 rated well in the various criteria in the AHP and changes to the weights of the main criteria of Operations Capability, Technical Performance, and ILS did not result

in rank reversal. This pointed to a robust decision outcome and indicated that R2C2 was a clear "winner" in the overall assessment based on the criteria developed.

For the other two systems, EC2 scored well in the area of ILS, as it had inherent advantages that place it ahead of System Y. As a result, an increase in the weights (and hence, importance) of ILS would serve to raise EC2 to a higher level, comparable to that of R2C2. However, it was unlikely that ILS would be accorded a weight of 45.7% to place it above Operations Capabilities.

7.2.8 AHP Conclusions and Recommendations

The survey and its feedback, the problem statement, and the COIs developed for R2C2 enabled the team to develop an AHP to identify the important factors for consideration in the analysis of alternatives. As a result of going through the set process of pair-wise comparisons and overall synthesis of results, the academic evaluation of the three possible candidates for the communication systems yielded R2C2 as the favorable system to adopt based on the criteria drawn up.

Though this serves as an illustrated academic example of the possibilities, the exercise could serve as a useful baseline or starting point for more elaborate studies or field tests to assess the performance of competing communication systems.

7.3 REQUIREMENTS TRAFFIC LIGHT CHART ANALYSIS

In addition to the AHP assessment of the JSIC EC2, System Y, and R2C2 system, each requirement was investigated to determine whether each system met the given requirements. There were three sets of requirements given for this project: CPD requirements, BAA requirements, and R2C2 team-generated requirements. For each requirement, all three systems were evaluated and color coded with green, yellow, or red. Green indicated that the system met the requirement. Yellow indicated a need for small modifications in order to accommodate the requirement, and red indicated a need for significant modification of the system. Table 27 shows the requirements that were met by all three systems. CPD requirements are written in red, BAA requirements are written in black, and R2C2 team-generated requirements are written in blue.

	JSIC EC2	System Y	R2C2
State of the art, agile, and self-contained			
Small footprint (physical)			
Transportable in commercial and military aircraft			
Collaboration via reachback			
Two-person transportable			
Marshall in 30 minutes			
Operational in 30 minutes			
Local physical storage (on one or more laptops)			
Transportable by commercial air or ground by two people			
Operable on standard electrical power			
Provide data and voice communications			
Support and training document			
Connect to commercial Internet			
Provide secure means (physical security, data security, and network security) of passing tactical information to supported commander for situation assessment.			
Provide compact, rugged, and mobile packaging.			
Provide flexibility for mission-dependent software and hardware configurations.			

Table 27: Traffic Light Chart (Accommodated)

Table 28 shows a set of requirements that were not met by one or more systems.

	JSIC EC2	System Y	R2C2
Satellite connectivity			
Able to operate in austere locations			
Two simultaneous data networks			
Secure wireless (objective)			
Utilize EoIP to include VTC			
Multi-mode operations (voice, data, and video simultaneously)			
Provide 1.024 Mbps threshold per network (4.196 Mbps objective)			
Provide capability of local and long haul communications.			
Provide means of collecting data from organic or inorganic assets.			
Provide self-supporting power supply in addition to capacity of operating on standard electrical power.			
Provide capability for operators to receive, display, analyze, filter, and pass simultaneous data from organic or inorganic assets.			

Table 28: Traffic Light Chart

Table 29 is a compilation of rationales behind the traffic light chart ratings in Table 28.

Satellite Connectivity	JSIC EC2 does not have a portable satellite dish. A minor modification of adding a satellite dish is needed.
Able to operate in austere locations	JSIC EC2 and System Y do not have a portable generator. A minor modification of adding a power generator is needed.
Two simultaneous data networks	JSIC EC2 is not capable of accessing CENTRIX and SIPRNet. A significant modification to its network architecture is needed.
Secure wireless (objective)	JSIC EC2 does not support a wireless capability. A minor modification to add wireless components is needed.
Utilize EoIP to include VTC	JSIC EC2 does not have a VTC device. A minor modification of adding the VTC devices is needed.
Multimode operations (voice, data, and video simultaneously)	JSIC EC2 does not accommodate video data. A minor modification of adding video camera is needed.
Provide 1.024 Mbps threshold per network (4.196 Mbps objective)	JSIC EC2 only utilizes INMARSAT satellite (L-band). L-band is not capable of 1.024 Mbps. A minor modification of utilizing Ku-band capable satellite dish is needed.
Provide capability of local and long haul communications.	JSIC EC2 and System Y do not have any local communication devices as a part of the system. A minor modification of adding a local communication module is needed.
Provide means of collecting data from organic or inorganic assets.	JSIC EC2 and System Y do not have organic data collecting devices. A minor modification of adding data collecting devices is needed (i.e., camera, video camera).
Provide self-supporting power supply in addition to capacity of operating on standard electrical power.	JSIC EC2 and System Y do not have a portable generator. A minor modification of adding a power generator is needed.
Provide capability for operators to receive, display, analyze, filter, and pass simultaneous data from organic or inorganic assets.	JSIC EC2 and System Y do not have data collecting personnel and local communication capability to wirelessly transmit the data to the operators. A significant modification is needed.

Table 29: Traffic Light Chart Considerations

In addition to ranking the three systems, this analysis was conducted to ensure that the R2C2 system met all of the CPD, BAA, and R2C2 team-generated requirements and that no vital aspects were left unanalyzed. The traffic light chart results were

consistent with the AHP analysis of the three systems that the R2C2 was again the most suitable system. R2C2 met 27 out of 28 requirements. System Y was ranked after R2C2 by meeting 22 out of 28 given requirements, and JSIC EC2 was ranked last by meeting only 16 requirements. A noticeable difference in the result between the AHP ranking and the traffic chart ranking is a change of place between the JSIC EC2 and System Y. This difference is due to slightly different criteria and weight assigned to each criterion. AHP covers the ILS aspect of the system that the requirement traffic light chart does not address. Moreover, each criterion of AHP is weighted based on their importance to the system, unlike equally weighted traffic light chart analysis.

While conducting the traffic light analysis, we discovered a few conflicting requirements. The first one addresses the number of operators. The CPD states that the system shall be operated by 4 operators, expanding up to 10; however, the BAA states that the system shall be operated by 5 clients, expanding up to 15. In order to resolve this conflict, the R2C2 team traced back to the scenario and investigated how many operators will be needed. Based on the scenario and operational experience of the R2C2 team members, the team concluded that 7-11 personnel are required for normal operations, including 3 security personnel to guard the system from physical intrusion and 4-8 operators in working in 6-hour rotations.

The second conflicting requirement concerned satellite communication capability. One of the CPD requirements states that DJC2 "shall provide limited Rapid Response communication capability to include SHF SATCOM, UHF TACSAT, INMARSAT, and handheld global satellite phone." The first noticeable redundancy in this requirement is the coexistence of INMARSAT and UHF TACSAT. UHF ranges from 300MHz to 3 GHz and includes P-, L-, and S-band. In order to provide low propagation attenuation and high tolerance of antenna pointing errors, INMARSAT also operates within the L-band. Employing INMARSAT when UHF TACSAT is available appears to be an unnecessary redundancy. The second questionable aspect of this requirement involves the addition of low-band UHF, which does not even meet the required minimum bandwidth of 1.024 Mbps. UHF might have been included by the requirement generators in order to increase overall communication link reliability by exploiting its higher tolerance of antenna-pointing errors and better propagation properties than SHF, or a

requirement to be interoperable with legacy systems. However, the R2C2 system satellite dish will be stationary and antenna-pointing accuracy will not be difficult to achieve. Moreover, in order to accommodate UHF capability into the system, another larger satellite dish will be required, and consequently will increase the weight and size of the system.

In summary, both INMARSAT and UHF TACSAT were concluded to be unnecessary capabilities of the system. SHF SATCOM was more than capable of handling what INMARSAT and UHF were designed to do without adding extra weight. A handheld global satellite phone will be utilized to provide a redundant SATCOM link, in addition to the SHF SATCOM for the purpose of increasing the overall link reliability of the system.

7.4 CONCLUSION

In the systems analysis phase of the SE process, time-critical R2C2 system architecture selected from the modeling phase was assessed for its suitability by using the AHP and traffic light comparison analysis. In the AHP, the analysis group identified critical issues R2C2 system will face in various operating scenarios and converted them into comparable criteria. Each criterion was then assigned a weight, based on the survey results, in order to signify its importance. The survey takers' profession did not affect the how he/she weighted each criterion and it was proven through the Kruskal-Wallis one-way analysis of variance. Hence, the 30 samples were considered to be from a homogenous source and overall results were computed. Such weights will provide valuable insights to the DJC2 program office on the relative importance of numerous criteria for this type of system. The R2C2 system was then compared with JSIC EC2 and System Y using the AHP and traffic light comparison. In both analyses, R2C2 was ranked as the most suitable system and one that met all but one requirement, as shown in Table 30.

	AHP	Traffic Light Matrix
R2C2	0.427	27/28
System Y	0.283	22/28
EC2	0.290	16/28

Table 30: Result of Three-System Evaluation

In summary, the analysis process provided the following valuable information:

- COIs, MOEs, MOSs, and MOPs to be used as a basis for future TEMP of the system.
- Relative importance between multiple criteria to be utilized to evaluate a rapid response C2 system.
- Proof that the R2C2 system was the best system to address present capability gaps and requirements for a rapid response C2 system.
- Analysis of existing requirements and modification suggestions to as-is and proposed systems.

APPENDIX A: SCENARIO COMPARISON

Scenario Comparison

		General Goals	Scenarios	Examples	Respond Time 1. Adequate (> 1 day) 2. Average (< 1 day) 3. Short (< 12hrs)	User expectation input (details/freq)	process	output (Detail/freq)
	War	Fight and Win	Combat Ops (Attack)	Deployment	3. short, due to plans to attack U. S. interst, intel is neede for counter-offensive attacks	high/high	high/moderate	very high/high
			Combat Ops (Defend)					
			Combat Ops (Blockade)					
MOOTW	POT	Deter War and Resolve Conflicts	Peace enforcement	Civil Unrest (eg., Ivory Coast)	3. Time is critical. Tensions are increasing and intel is needed to determine scope of operations	High/Very High	High/Moderate	High/Moderate
			Noncombatant Evacualtion Operations (NEO)					
			Strikes/Raids	Counter-terrorism (eg., terrorism off southern phillipines)	1. adequate, caution must be taken to prevent detection	high/high	moderate/moderate	high/moderate
			Show of forces					
			Counterterrorism					
			Peace Keeping					
			Counterinsurgency					
	Peace	Promote Peace, Support Law and Order	Anti-terrorism	Disaster relief (eg., South America)	3. time is critical, need to be inserted quickly for intel gathering	high/high	low	high/moderate
			Disaster relief					
			Peace building					
			Counter-drug	Pandemic (eg., Bird Flu)	1. Adequate. Should have ample time to access conditions (situations develop)	moderate/high	low	low/moderate
			Domestic support					
			Pandemic control					

Complexity of Operation	Environment 1. Peaceful; 2. Tension; 3. Hostile			Infrastructure (e.g., power supply, shelter and basic needs for px)	Probability of Occurrence	Impact
1. Small (2 px) 2. Medium (platoon) 3. Large (company and beyond)	Counter IA	Troop Safety	Political Sensitivity	1. Supported 2. Supplementary 3. Poor	1. Low 2. Medium 3. High	1. Localize 2. Regional 3. Widespread
3. Medium	2. Tension	3. Hostile	3. Hostile	1. Supported	1. Low	3. Widespread (this war will involve other nations)
3. Large 2-10 man teams	2. Tension	3. Hostile	2. Tension	2. Supplementary	2. Medium growing tensions, current attacks on UN troops	2. Regional UN involvement and former French colony with French interest
2. Medium	3. Hostile	3. Hostile	2. Tension	3. Poor	3. High	1. Localize
2. Medium	1. Peaceful	2. Tension	1. Peaceful	3. Poor	3. High	1. Localize to disaster site
2. Medium	1. Peaceful	1. Peaceful	1. Peaceful	1. Supported	1. Low	3. Widespread (virus may spread from human to human)

Stakeholders	Trafficability	Duration (stay + ops time)	Prior Intel/Info	Special
1. Intra-agency 2. Inter-agency 3. Coalition	**1. Supported 2. Supplementary 3. Poor**	**1. Short (<1 wk) 2. Med (<1 mth) 3. Long (>1 mth)**	**1. Not required 2. Is a bonus 3. Necessary**	**1. None 2. Some resources/efforts 3. Lots of resources/efforts**
Coalition	1. Supported	2. Med (initial SA and intel should be sufficient depending on Country X's time line)	3. Necessary (best place to set up and location of leadership)	If no Middle Easterners available to conduct mission probability of success is greatly reduced Local support would be a bonus
3. Coalition(UN, France, NGO)	2. Supplementary hazardous conditions in Northern region (roadblocks, check points…)	1. Short intel is critical before follow on troops will be deployed to support the government	3. Necessary for air drop to the North and rebel locations	
3. Coalition	2. Supplementary	2. Med (determining location of terrorist may take a few weeks)	2. Is a bonus (the more we have the less time to complete mission)	The level of complexity is high, terrorist protection may cause additional complexity
3. Coalition (include various countries coming to help)	3. Poor	3. Long (till host is self-sustain)	3. Necessary (pt of insertion, factors that affect ops plan, has situation stabilise)	Potential of being sabotage in "peaceful" environment,
3. Coalition (include various countries coming to help)	1. Supported	3. Long (till the pandemic gets contain)	3. Necessary (preventive measures prior insertion) intel need to safe guard operators (inserted troop)	Potential of being sabotage in "peaceful" environment

THIS PAGE INTENTIONALLY LEFT BLANK

OP 2.2 Collect and Share Operational Information

To gather information from operational and tactical sources on operational and tactical threat forces and their decisive points (and related high-payoff targets such as CBRNE weapon production, infrastructure and delivery systems). It also includes collection of information on the nature and characteristics of the operational area (including area of interest). Locating and reporting captured or isolated personnel falls under this task. In addition, collection of data to support combat assessment is included in this task. The sharing of collected information within the multi-Service intelligence communities can consolidate return of information, promote fusion, and prevent retasking of scarce assets. This task applies in peace and war and those MOOTW. It includes the sharing of collected information among all DOD organizations and non-DOD agencies in support of Homeland Security. All intelligence activities will be executed in accordance with Intelligence Oversight.

OP 2.2.1 Collect Information on Operational Situation

To obtain operationally significant information on enemy (and friendly) force strengths and vulnerabilities, threat operational doctrine, and forces (land, sea, and air and space). Threat includes threat allies, and, in MOOTW, insurgents, terrorists, illegal drug traffickers, belligerents in peace support or peace enforcement situations, and other opponents. It also includes collecting information on the nature and characteristics of the area of interest, to include collecting battlefield damage assessment, munitions effects, medical assessments, and hazards, such as CBRNE contamination to conduct mission assessment. The nature and characteristics of the area include significant political, economic, industrial, geospatial (e.g., aeronautical, hydrographic, geodetic, topographic), demographic, medical, climatic, and cultural, as well as psychological profiles of the resident populations. This task includes collecting counterintelligence information to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or persons, or international terrorist activities.

OP 4 Provide Operational Logistics and Personnel Support

To provide logistics and personnel support activities required to sustain the force in campaigns and major operations within the joint operations area. The logistic concept should support theater activity by properly organizing support from the CONUS base to the combat zone. At the theater operational level, specific considerations include identification of operational requirements and establishment of priorities for the employment of the resources provided. This theater of operations/joint operations area

sustaining base, which includes the communications zone (COMMZ), links strategic sustainment to tactical CSS. In military operations other than war, the activities under operational support also pertain to support of US forces, other USG agencies, and forces of friendly countries or groups being supported by US forces. Operational support includes sustaining the tempo and the continuity of operations throughout a campaign or major operation. This task includes obtaining sustainment support from sources other than Military Services and includes the following: host-nation support, logistic civil augmentation, DOD civilian support, and captured materiel.

OP 5.1.9 Coordinate Information Assurance (IA) Procedures

To coordinate IA procedures established by the JFC for forward deployed operations.

SN 1 Conduct Strategic Deployment and Redeployment

To conduct the relocation of forces to desired theaters and their return in accordance with national military strategy and OPLANs to include within CONUS in support of Homeland Security missions. This task focuses on the movement of forces and resources from a point of origin to a specific operational area. Strategic deployment encompasses relocation of forces, equipment, and supplies to a theater from CONUS, or from one theater to another, for subsequent reception, staging, onward movement, and integration (RSOI). This task applies to mobilization and non-mobilization situations. Forces include air, land, and sea forces, as well as special operations forces.

SN 1.2 Conduct Deployment and Redeployment

To move forces and cargo in accordance with both national strategic and theater strategic requirements and in conformance with the supported commander’s concept of operations.

SN 2.2 Collect Strategic Information

To exploit sources of strategic information and to deliver the intelligence obtained to the appropriate processing organization for use in producing strategic intelligence. Strategic surveillance and reconnaissance are related to this task as is counterintelligence.

SN 2.4.1 Evaluate, Integrate, Analyze, and Interpret Information

To appraise information for credibility, reliability, pertinency, and accuracy (evaluate). It includes forming patterns through the selection and combination of

processed information (integrate). The task further includes reviewing information to identify significant facts for subsequent interpretation (analyze). Finally, the task is to judge the significance of information in relation to the current body of knowledge (interpret).

SN 3.3.6.1 Assess Critical Infrastructure (CI) Impacts to Operational Capability

Determine the operational impacts resulting from the loss, disruption, and/or degradation of mission critical infrastructure.
Note: This task includes identifying the critical infrastructure and assets that are components of systems supporting all assigned missions; analyzing the potential consequences of a global event; assessing potential impacts to critical infrastructure and assets supporting assigned missions; and reporting results of the analysis and assessment.

SN 4.4 Reconstitute National Forces and Means

To reconstitute the Armed Forces of the United States that will counter any emerging global threat. National reconstitution involves forming, training, and fielding new fighting units. This task includes initially drawing on cadre-type units and laid-up military assets, mobilizing previously trained or new manpower, and large-scale use or employment of the industrial base. This task also involves maintaining technology, doctrine, training, experienced manpower (military, DOD civilian, and contractors), and the innovative approach necessary to retain the competitive edge in decisive areas of potential military competition. This task includes providing the support required for reconstituting a host-nation's forces in military operations other than war.

SN 5.1.2.1.4 Provide Global Communications and Networks for Video Services

To provide global video service capabilities, ranging from network delivery of video of live events and real time video communications sessions among people who are geographically dispersed to delivery of video from prerecorded video files.

SN 5.1.2.1.5 Provide Global Voice Communications and Networks

To provide global voice services through telephone networks and satellite-based personal communications systems.

SN 5.1.2.2.3 Provide Collaborative Applications and Services

To provide collaborative tool applications to enhance simultaneous access to real-time information and enable two or more operational users to simultaneously collaborate without the need to be co-located.

SN 5.1.2.3.4 Provide Data Storage

To provide and administer data storage for both classified and unclassified environments.

SN 5.1.2.8 Operate Computing Centers, Applications, Services, Systems and Networks

To administer and operate computing centers, systems and networks to satisfy the needs of the warfighter.

SN 5.5.2 Conduct Defensive Information Operations

To perform authorized actions to protect, monitor, analyze, detect, and respond to unauthorized activity within national security information systems and computer networks. (Executive Order 12333, Chairman's Memorandum, CM- 573-88, National Security Directive, National Policy for the Security of Telecommunications and Information)

SN 6 Conduct Mobilization

To expand the Armed Services by assembling and organizing national resources to support national objectives in time of war or other emergencies. This task brings the Armed Services, or part of them, to a state of readiness for war or another national emergency. This task includes advising the Secretary of Defense on mobilization. It includes activating all or part of the Reserve Components (RC), as well as assembling and organizing personnel, supplies, and materiel. This task is performed when the Secretary of Defense initiates a selective, partial, full, or total mobilization. Mobilization tasks of combatant command components are included under this joint task. For example, US Army Pacific (USARPAC), a component command of US Pacific Command (USPACOM), has mobilization responsibilities. These mobilization responsibilities are analyzed under the national strategic level (rather than a theater strategic task) because USARPAC performs these responsibilities as a major Army command (MACOM). Thus, USARPAC is considered to be performing national military functions. However,

USARPAC reports mobilization status through the combatant command as well as the Service.

SN 6.2 Alert Forces for Mobilization

To transition the force from reserve to active duty status with available personnel and facilities, and to complete all administrative and processing actions. The alert phase begins when units or individuals receive notice of pending order to active duty and ends when the unit enters active Federal service.

SN 6.2.1 Alert Units and Individuals of Pending Mobilization

To provide readiness for action—the period of time during which troops standby in response to an alarm. This task includes any form of communication used by Service headquarters or other competent authority to notify National Guard and Reserve unit commanders that orders to active duty are pending.

SN 8.1.7 Coordinate Information Sharing Arrangements

To arrange for the selected release and disclosure of unclassified and classified information in support of multinational operations and exercises. This task may involve coordination with national intelligence agencies, law enforcement agencies (down to the state and local levels), and the Department of State.

ST 5.1.6 Establish Information Assurance (IA) Procedures

To establish information assurance procedures for deployed operations. This task includes developing IO appendices including defensive IO and IA for all deliberate plans and operations orders as required. IA may be used to ensure information and information systems availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

ST 6.2.6 Establish and Coordinate Security Procedures for Theater Forces and Means

To enhance freedom of action by reducing the vulnerability of friendly joint forces to hostile acts, influence, or surprise. This task includes measures to protect forces from surprise, hostile observation, detection, interference, espionage, and sabotage. This

activity also includes protecting and securing the flanks in joint operations and protecting and securing critical installations, facilities, systems and air, land, and sea LOCs. It includes antiterrorism to protect the morale of the force and enhance the legitimacy of host-nation forces.

ST 6.3 Secure Theater Systems and Capabilities

To protect friendly systems and capabilities by identifying threats and reducing or compensating for vulnerabilities.

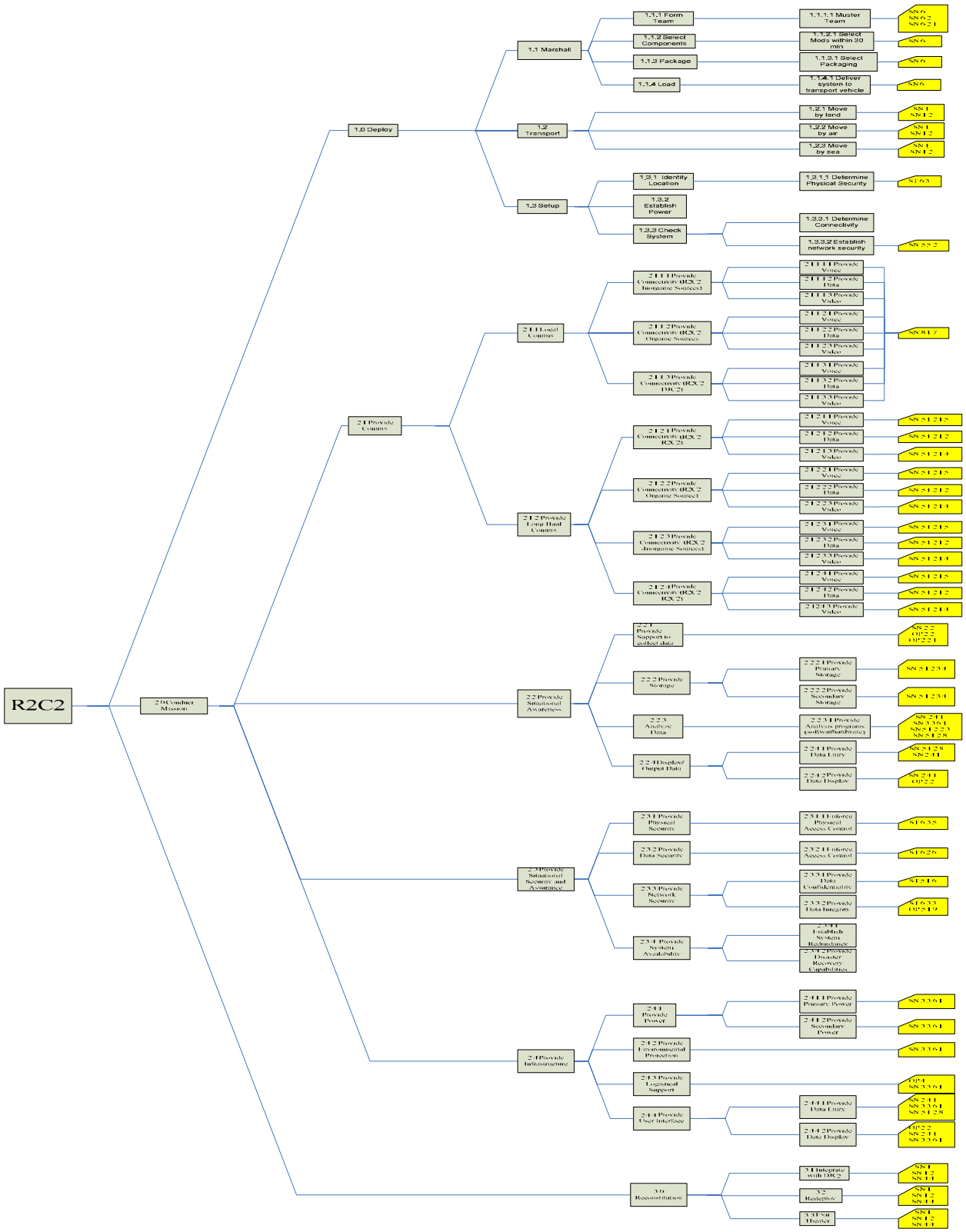
ST 6.3.3 Supervise Communications Security (COMSEC)

To supervise the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications. COMSEC includes crypto security, transmission security, emission security, and physical security of communications security materials and information.

ST 6.3.5 Protect Theater Information Systems

To coordinate theater-wide activities to protect and defend information and information systems. This task includes integrating and synchronizing indigenous and joint force capabilities for defensive IO, ranging from technical security measures (such as INFOSEC) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes). Information assurance includes producing the theater policies and procedures designed to ensure availability, integrity, authenticity, confidentiality, and non-repudiation of information. Information system defense includes defensive measures, detection and reporting of attacks or intrusions, and the initiation of restoral and response processes.

APPENDIX C: R2C2 FLOWCHART


R2C2
2.0 Conduct Mission
1.0 Deploy
1.1 Marshall
1.1.1 Form Team
1.1.1.1 Muster Team
SN 6
SN 6.2
SN 6.2.1
1.1.2 Select Components
1.1.2.1 Select Mods within 30 min
SN 6
1.1.3 Package
1.1.3.1 Select Packaging
SN 6
1.1.4 Load
1.1.4.1 Deliver system to transport vehicle
SN 6
1.2 Transport
1.2.1 Move by land
SN 1
SN 1.2
1.2.2 Move by air
SN 1
SN 1.2
1.2.3 Move by sea
SN 1
SN 1.2
1.3 Setup
1.3.1 Identify Location
1.3.1.1 Determine Physical Security
SI 6.3
1.3.2 Establish Power
1.3.3 Check System
1.3.3.1 Determine Connectivity
1.3.3.2 Establish network security
SN 8.5.2
2.1 Provide Comms
2.1.1 Local Comms
2.1.1.1 Provide Connectivity (R2C2 Inorganic Sources)
2.1.1.1 Provide Voice
2.1.1.2 Provide Data
2.1.1.3 Provide Video
2.1.1.2 Provide Connectivity (R2C2 Organic Sources)
2.1.2.1 Provide Voice
2.1.2.2 Provide Data
2.1.2.3 Provide Video
SN 8.1.7
2.1.1.3 Provide Connectivity (R2C2 DSC)
2.1.3.1 Provide Voice
2.1.3.2 Provide Data
2.1.3.3 Provide Video
2.1.2 Provide Long Haul Comms
2.1.2.1 Provide Connectivity (R2C2 R2C2)
2.1.2.1 Provide Voice
SN 8.1.2.1.5
2.1.2.2 Provide Data
SN 8.1.2.1.2
2.1.2.3 Provide Video
SN 8.1.2.1.1
2.1.2.2 Provide Connectivity (R2C2 Organic Sources)
2.1.2.2.1 Provide Voice
SN 8.1.2.1.5
2.1.2.2.2 Provide Data
SN 8.1.2.1.2
2.1.2.2.3 Provide Video
SN 8.1.2.1.1
2.1.2.3 Provide Connectivity (R2C2 Inorganic Sources)
2.1.2.3.1 Provide Voice
SN 8.1.2.1.5
2.1.2.3.2 Provide Data
SN 8.1.2.1.2
2.1.2.3.3 Provide Video
SN 8.1.2.1.1
2.1.2.4 Provide Connectivity (R2C2 R2C2)
2.1.2.4.1 Provide Voice
SN 8.1.2.1.5
2.1.2.4.2 Provide Data
SN 8.1.2.1.2
2.1.2.4.3 Provide Video
SN 8.1.2.1.1
2.2 Provide Situational Awareness
2.2.1 Provide Support to collect data
SN 2.2
OP 2.2
OP 2.2.1
2.2.2 Provide Storage
2.2.2.1 Provide Primary Storage
SN 8.1.2.3.4
2.2.2.2 Provide Secondary Storage
SN 8.1.2.3.4
2.2.3 Analyze Data
2.2.3.1 Provide Analysis programs (software/hardware)
SN 2.4.1
SN 3.3.6.1
SN 8.1.2.3
SN 8.1.2.8
2.2.4 Display/ Output Data
2.2.4.1 Provide Data Entry
SN 8.1.2.8
SN 2.4.1
2.2.4.2 Provide Data Display
SN 2.4.1
OP 2.2
2.3 Provide Situational Security and Assurance
2.3.1 Provide Physical Security
2.3.1.1 Enforce Physical Access Control
SI 6.3.5
2.3.2 Provide Data Security
2.3.2.1 Enforce Access Control
SI 6.2.6
2.3.3 Provide Network Security
2.3.3.1 Provide Data Confidentiality
SI 5.1.6
2.3.3.2 Provide Data Integrity
SI 6.3.3
OP 5.4.9
2.3.4 Provide System Availability
2.3.4.1 Establish System Redundancy
2.3.4.2 Provide Disaster Recovery Capabilities
2.4 Provide Infrastructure
2.4.1 Provide Power
2.4.1.1 Provide Primary Power
SN 3.3.6.1
2.4.1.2 Provide Secondary Power
SN 3.3.6.1
2.4.2 Provide Environmental Protection
SN 3.3.6.1
2.4.3 Provide Logistical Support
OP 1
SN 3.3.6.1
2.4.4 Provide User Interface
2.4.4.1 Provide Data Entry
SN 2.4.1
SN 3.3.6.1
SN 8.1.2.8
2.4.4.2 Provide Data Display
OP 2.2
SN 2.4.1
SN 3.3.6.1
3.0 Reconstitution
3.1 Integrate with DSC
SN 1
SN 1.2
SN 1.4.1
3.2 Redeploy
SN 1
SN 1.2
SN 1.4.1
3.3 Exit Theater
SN 1
SN 1.2
SN 1.4.1

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: SATELLITE SYSTEMS

Sat System	Bands			Weight		Stowed Dimensions	Transmit Rate	Receive Rate	Set up Time	Power Consumption	MIL-STD *estimate*	iDirect	Licenses	Cost (single unit)
	X	***Ku***	***Ka***	***lbs***	***# of cases***	***inches***	***Mbps***	***Mbps***	***min***	***W AC***				
Norsat Globetrekker	Optional	Yes	Optional	<50	1	19.5 x 27x 13.2	4	4	<10	480	$100,000.00	Supports	Pending (none)	*estimate*
Norsat U.P. 5200	Optional	Yes	Optional	46/46	2	16 x 11 x 25/ 16 x 11 x 25	8.448	8.448	10	480	$100,000.00	Supports	Pending (FCC, Intelsat)	$100,000.00
SWE-DISH IPT-i Mil Suitcase	Yes	Yes	Optional	86	1	27.6 x 18.5 x 12.2	4	4	5	650	$110,000.00	Supports/ Integrated	Intelsat, Eutelsat, Hispasat, Europestar, IPStar, Shin Sat, AsiaSat FCC	$100,000.00
TCS DVM-90	No	Yes	No	40	1	carry-on	2.4	2.4	20	500	~	Supports	Pending (none)	$110,000.00
GSI GlobeComm Auto-Explorer (.77m)	No	Yes	No	48/50	2	22x14x10/ 22x14.11	4.2	4.2	15	375	~	Supports/ Integrated	Intelsat, Panamsat, Eutelsat	~
														~

LIST OF REFERENCES

"A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues," 8 December 2005, http://www.cbo.gov/ftpdocs/69xx/doc6946/12-08-BirdFlu.pdf.

Aczel et al., "Procedures for Synthesizing Ratio Judgments," *Journal of Mathematical Psychology*, 1983.

Bailey, C., "Reference Department of Defense Usage of FalconView™," [http://www.falconview.org/events.htm], March 2006.

BBC News, Country Profile: Ivory Coast, http://news.bbc.co.uk/1/hi/world/africa/country_profiles/1043014.stm.

Blanchard, B.S. and Fabrycky, W.J., *Systems Engineering and Analysis*, 3rd Edition, pp. 48-50, Prentice Hall, 1998.

Bolloju, N., "Aggregation of Analytic Hierarchy Process Models Based on Similarities in Decision Makers' Preference," *European Journal of Operational Research*, 2001.

Burns, R.N., "United States Policy Toward Iran," Opening Statement before the House International Relations Committee, 8 March 2006.

Chairman, Joint Chiefs of Staff, *Manual 3500.04D*: *Universal Joint Task Lists (UJTL)*, 1 August 2005.

Chairman, Joint Chiefs of Staff, Joint Warfare of the Armed Forces of the United States, Joint Pub 1 (Washington, D.C.: 14 November 2000), VI-5, CJCS Posture Statement before the 106th Congress Committee, On Armed Service, United States Senate, 8 February 2000.

Chairman, Joint Chiefs of Staff, Joint Publication 3-0: Doctrine for Joint Operations, Chapter 1 "The Strategic Context," September 2001.

Chairman, Joint Chiefs of Staff, Joint Publication 6-0: Joint Communications System, 20 March 2006, pp. 11-10.

Coalition Operating Area Surveillance and Targeting System 2006 Overview.

Condon et al., "Visualizing Group Decisions in the Analytic Hierarchy Process Models," *Computers and Operations Research*, 2003.

Cupp, J., Sgt., USA, USJFCOM Public Affairs, "Ainsworth Honored as Command's Joint Junior Officer of the Quarter," 2 March 2006, http://www.jfcom.mil/newslink/storyarchive/2006/pa030206.htm, May 2006.

Cupp, J., Sgt., USA, USJFCOM Public Affairs, "New Suffolk Facility to Provide Warfighter Rapid Solutions," 10 September 2004, http://www.jfcom.mil/newslink/storyarchive/2004/pa091004.htm, May 2006.

Defense Update News Commentary, "Iran's National Deterrent: Weapons of Mass Destruction Program," http://www.defense-update.com/2004/04/irans-national-deterrent-weapons-of.html, April 2004.

DJC2 Broad Area Announcement FBO: DON-SNOTE-05-0624-002, 24 June 2005.

DJC2 Capabilities Production Document OPNAV N71C2- 688(1)-71-05, 30 November 2005.

DoD Directive 8500.1, "Information Assurance," 24 October 2002.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," 6 February 2003.

Forman et al., "The Analytic Hierarchy Process – An Exposition," *INFORMS*, Vol. 49, No. 4, 2001.

Free Travel Tips, "Luggage Information," http://www.freetraveltips.com/Airlines/air03.htm, May 2006.

Gabriel, C., "Wi-Max: The Critical Wireless Standard," BluePrint Wi-Fi Report I, p. 4, 1 October 2003.

Global Security.org: Ivory Coast Conflict, http://www.globalsecurity.org/military/world/war/ivory-coast.htm.

Globalstar, Inc. Company Website, http://www.globalstar.com, April 2006.

Groove Networks Website, www.groove.net, March 2006.

GSI GlobeComm, Auto-Explorer Brochure, http://www.globecommsystems.com/pdf/0.77%20Auto%20explorer.pdf, April 2006.

Harris, "Secure Communications Solutions," http://www.govcomm.harris.com/secure-comm/, May 2006.

Honda, "Super Quiet Inverter Generators," http://www.hondapowerequipment.com/gensup.asp, May 2006.

iDirect, "iDirect Technologies Broadband VSAT System – Summary," www.idrect.net, May 2006.

"Information Assurance Technical Framework (IATF)," National Security Agency, Release 3.1, September 2002.

Inmarsat Company Webpage, http://government.inmarsat.com/solutions/default.aspx, April 2006.

Interview between Gary Langford, Dr, Professor, NPS and James Colgary, ENS, NPS, 1 March 2006.

Interview between Johnny Hill, Capt, USAF, 86th Space and Communications Squadron, Kaiserslautern, Germany and authors, 12 April 2006.

Interview between Kevin Stoffell, Capt, USMC, Student, NPS and James Colgary, ENS, Student, NPS, 29 March 2006.

Interview between the DJC2 JPO and the R2C2 team, 29 March 2006.

IP Access, "Nano BTS," http://www.ipaccess.com/products/nanoBTS.htm, March 2006.

Iridium Satellite Company Website, http://www.iridium.com, March 2006.

Kuppuswamy, C.S., "Abu Sayyaf: The Cause for the Return of U.S. Troops to Philippines," South Asia Analysis Group Paper, No. 417, 28 February 2002.

Lancaster, D.D., "Developing a FLy-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)," Master's Thesis, Naval Postgraduate School, Monterey, CA, June 2005.

Lee, T.H., "An Analysis of Emerging Commercial Wide Band Satellite System and their potential for military use," http://handle.dtic.mil/100.2/ADA361515., April 2006.

Luggage Pros, "Luggage Restrictions," http://www.luggagepros.com/policies/luggage-restrictions.shtml, May 2006.

McHale Backpacks, http://www.mchalepacks.com/packs/detail/MBSuper.htm, May 2006.

Mobile Computing Definitions, "PAN," http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html, May 2006.

Morrison, D., "Micro Fuel Cell Demonstrates High Power Output," http://powerelectronics.com/news/fuel-cell-output/, May 2006.

Negroponte, J.D., Director of National Intelligence, "Threats, Challenges, and Opportunities for the U.S.," Annual Threat Assessment to the Senate Select Committee on Intelligence, 2 February 2006.

News@AsiaOne, 5 April 2005, Singapore outlines flu pandemic preparedness plans; to holdemergency drill, http://hosted.ap.org/dynamic/stories/A/AS_MED_ SINGAPORE_ FLU_ PREPAREDNESS_ASOL-SITE=ASIAONE&SECTION =SOUTHEAST &TEMPLATE.

Norsat, UP 5200 Brochure, http://www.norsat.com/pdf/download/Norsat%205200Ku-10W-P3K.pdf, April 2006.

Norsat, Norsat Globetrekker Brochure, http://www.norsat.com/pdf/download/UPT.pdf, April 2006.

Pelican Cases, http://www.pelican.com/cases_detail_specs.php?Case=1600, May 2006.

Perea, D., "Missed Signals," *Government Executive*, pp. 53-56, February 2006.

Quadrennial Defense Review, 6 February 2006, p. vii.

Rasmussen, E., MC, USN, "Assessing Information Support at the Civil-Military Boundary, Operation Unified Assistance in Indonesia," January 2005.

Red Cross Red Crescent Operations Update, http://www.ifrc.org/cgi/pdf_appeals.pl?01/ 020118.pdf.

Report on Naval Postgraduate School response to the 2004 Southeast Asia Tsunami, "Hastily Formed Networks for Complex Humanitarian Disasters and Emergencies," 25 July 2005.

Saaty, T.L., "Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World," RWS Publications, 1990.

Scurry, B., "Mobile User Objective System (MUOS)," Presentation given at the Norfolk Convention Center, 29 June 2005.

SolarSense, "Nomad 1500 Pro Series," http://www.solarsense.com/Products/ 1-Complete_Systems/3-NOMAD_1500/NOMAD_1500.html, May 2006.

Southwest Windpower, "Whisper 100/200 Specficication Sheet," http://www.alpinesurvival.com/Whisper_100_200_Spec_Sheet.pdf, May 2006.

Strong Angel III, San Diego, CA, 20-26 August 2006, Overview, Hosting Requirements, and Task List, 16 January 2006.

SWE-DISH, SWE-DISH IPT-I Mil Suitcase Brochure, http://www.swe-dish.se/upload/_PDF/SWE-DISH%20IPT%20MIL%20Suitcase%202006.pdf, April 2006.

Taylor, C. and Alves-Foss, J., "MILS Multiple Independent Levels of Security," 8 December 2005, http://www.acsac.org/2005/case/thu-130-taylor.pdf.

TeleCommuncations Systems, TCS DVM90 Brochure, http://www.telecomsys.com/downloads/government/pdf/brochure_DVM90.pdf, April 2006.

Telephone conversation between Mr. Harry, Camp Roberts, STEP Site Operations Technician and Lisa Sullivan, LCDR, Student, NPS, 15 May 2006.

Terrorism: Question and Answer, Council on Foreign Relations, Abu Sayyaf Group: Philippine, Islamist Separatists, http://cfrterrorism.org/groups/abusayyaf2.html.

The Joint Interoperability Test Command, "Combined Enterprise Regional Information Exchange System (CENTRIXS)," http://jitic.fhu.disa.mil/washops/jtca/centrix.html, May 2006.

Time Critical Targeting, http://www.dtic.mil/ndia/2002interop/morehouse.pdf, June 2006.

TNT Overview Report, 2006.

Toresse, J., Jr., "Basilan: Abu Sayyaf's Birthplace," http://www.abs-cbnnews.com/images/news/microsites/abusayyaf/basilan.htm.

United States Department of Defense, MIL-STD-1472F (DoD), Department of Defense Design Criteria Standard, Human Engineering, 23 August 1999.

United States Joint Chiefs of Staff, *Joint Communications System*, Joint Pub 6-0, Washington, DC: 20 March 2006, pp. III 18-III 20.

United States Joint Chiefs of Staff, *Joint Doctrine for Military Operations Other Than War*, Joint Pub 3-07, Washington, DC: 19 June 1995, p. IV-4.

United States Department of State, http://travel.state.gov/travel/cis_pa_tw/cis/cis_1109.html.

United States Geological Survey, http://earthquake.usgs.gov/regional/world/central_america/density.php.

Valence Technology, Inc., "Why compromise military safety with traditional Lithium-ion batteries?" http://www.valence.com/pdffiles/Military_Datasheet.pdf, May 2006.

White, R.A., Seismic History of the Middle America Subduction Zone Along El Salvador, Guatemala, and Chiapas, Mexico: 1526–2000, Manuscript Accepted 16 June 2003, http://www.gsajournals.org/gsaonline.

Wikipedia, "802.ll," http://en.wikipedia.org/wiki/802.11b, March 2006.

Wikipedia, "Computer Storage," http://en.wikipedia.org/wiki/Digital_Storage, May 2006.

World Health Organization, Avian Influenza: Assessing the Pandemic Threat, (Geneva: World Health Organization, January 2005).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library (Code 013)
   Naval Postgraduate School
   Monterey, CA 93943-5002

3. Deployable Joint Command and Control (DJC2)
   Joint Program Office
   Panama City, FL 32407-7001