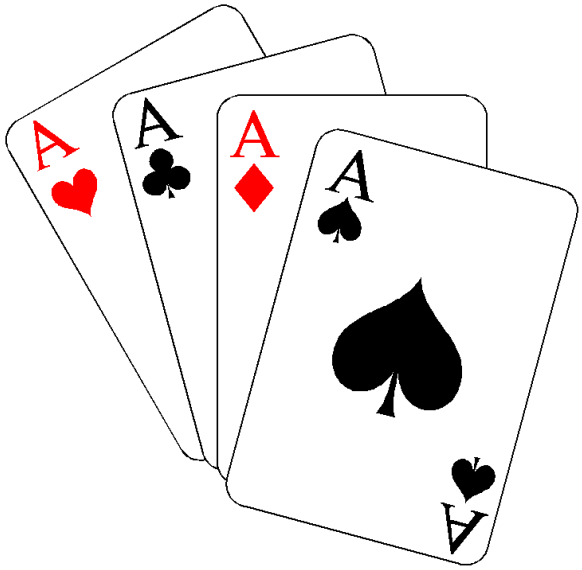
Air Traffic Controller
Cyber Attack Evaluation Serious Game
(ACES)



ACES Final Report

Spring Semester 2014

OR/SYST 699 Capstone Project

George Mason University

Fairfax, Virginia

THIS PAGE INTENTIONALLY LEFT BLANK

SIGNATURE PAGE

Submitted by _____ Date: _____

Doran Cavett, SOER Team
MSSE Candidate

Submitted by _____ Date: _____

Imran Shah, SEOR Team
MSOR Candidate

Submitted by _____ Date: _____

Wilbert C. Fontan, P.E., SEOR Team
MSSE Candidate

Concurred by _____ Date: _____

Paulo CG Costa, PhD
Sponsor, GMU C4I Center

Concurred by _____ Date: _____

Christopher Ondrus
Sponsor, GMU Simulation & Game Institute

Approved by _____ Date: _____

Kathryn Blackmond Laskey, PhD
Professor, OR/SYST 699

Executive Summary

The security and economic prosperity of a nation depend on critical infrastructure that is increasingly at risk from a variety of hazards, including cyber-attacks. Increasing connectivity and automation of critical infrastructure components and processes results in vulnerability to attacks on the cyber-infrastructure supporting our automated processes. This creates an opening for hostile actors to disrupt society through cyber-attacks. Progressively more, the cyber domain is seen as a new dimension of warfare — one that is especially open to lightweight, agile actors who do not require resources for major hardware investments and can operate from remote locations to disrupt our critical infrastructure.

The security and resilience of these assets, systems, networks, and functions — whether physical or cyber — requires a partnership that involves individuals and communities, businesses and non-profits, schools and universities, and governments at all levels, as well as a clear understanding of the risks we face. Only together, they can build a better understanding of the potential mission impacts of hostile cyber operations, better processes for planning for and rapidly responding to cyber threats, and better ways to assess both the impact of cyber operations and the effectiveness of their responses.

Serious games provide a means to evaluate cyber-attacks against critical infrastructure without the need for large investments in real world test scenarios and the potential harm or loss of life. A team of graduate students from the George Mason University (GMU) Systems Engineering and Operations Research Department (henceforth the SEOR Team) will guide and assist a cadre of GMU Simulation and Gaming Institute (SGI) students throughout the design, development, and proof of concept phases of a serious game based on the contents of three produced documents: The Concept of Operations document, the System / Subsystem Specification Document, and the Software Design Document. Phases or milestones not completed by the end of the Spring 2014 semester should be considered as potential themes for future collaborative efforts between both the organizations.

The Air Traffic Controller Cyber-attack Evaluation Serious (ACES) game will simulate cyber-attacks onto the Air Traffic Management (ATM) system used to conduct offshore helicopter operations in support of oil production off the Rio de Janeiro coast of Brazil. ACES will provide a venue for training Air Traffic Controllers (ATC) and understanding the impacts of cyber-attacks on ATM infrastructure and operations which will in turn help them identify and prepare effective mitigating actions.

Table of Contents

Table of Figures

List of Tables

1 Introduction

For the Spring 2014 semester our team was assigned the task to investigate the ability to extend work completed in the Fall of 2013 within the George Mason University (GMU) Command, Control, Communications, Computers, and Intelligence (C4I) Center that dealt with "measuring the cyber impact on a mission using overall effects, without knowing the enemies plans" developed by Lieutenant Colonel (LtCol) Alexandre Barreto PhD. He took his hypothesizes and his goals and applied it to the oil field operations within the Campos Basin Region of Rio De Janeiro, Brazil because of his affiliation with the Brazilian Air Force and interest in expanding the domain knowledge in the cyberspace area for his country.

The Campos Basin Region that Dr. Barreto started his research on is critical to the state of Brazil because it accounts for roughly 80% of the petroleum production that is produced and is a reliable revenue stream for the country. Since the majority of the oilfields reside approximately 2000 meters offshore in a small set of islands the country has chosen to utilize Automatic Dependent Surveillance-Broadcast (ADS-B) Technology. ADS-B technology is much cheaper than conventional RADAR systems and consists of relay stations that broadcast an aircraft's Global Positioning System (GPS) location to a central RADAR station for display on an Air Traffic Controller's (ATC) display. ADS-B is also known to be a more accurate method for locating and positioning aircraft. The ability to know the location of aircraft more precisely allows for ATCs to better position aircrafts in the sky and reduces congestion in airports. The ADS-B system consists of the relay towers as well as a component that gets installed on aircrafts that translates and broadcasts a vehicle's position along with a unique identifier to the ATC Tower, the only problem with the technology is that it is susceptible to cyber-attacks.

The vision for our project was to leverage the work completed by LtCol Barreto and turn his simulation work into a serious game. In theory this would allow for the tool to be used in training Air Traffic Controllers in identifying cyber-attacks, procedures for dealing with a cyber-attack, and mitigation strategies for intercepting cyber-attacks. Another area in which the serious game could be expanded is to study the overall effects of cyber-attacks on computing components and the associated costs that are incurred because of the attacks. These are all areas that our team has taken into account when thinking about the structure of our solution and the possibility of expansion of the tool beyond this semester's work.

Throughout the semester we've realized that we have been lucky enough to work with the visionaries of the notion and had also been given the opportunity to partner with the newly formed Simulation and Gaming Institute (SGI) at GMU to combine our skillsets and work towards a common goal in the creation of the serious game. We found that the project has high hopes and demands but at the same time the vision is quite achievable given the skills

required that resources that GMU offers. Throughout this paper we will provide our recommendations for needed resources, speculated timelines, modifications to the existing architecture, our process for development of a Concept of Operations (CONOPS), our development process for System Requirements, and our analysis of the integration of the proposed software tools and their capabilities.

1.1 Project Team

The project team was divided up into three distinct groups for our effort; there was the Project Sponsor group, the SGI group, and the Systems Engineering and Operations Research (SEOR) group. The SGI and SEOR groups worked together while the Sponsor provided the early vision, concept, and reviewed our documents and critiqued our ideas and proposed solution. Overall the team possessed a good set of skills to start an investigation into constructing the serious game and determining a forward path.

1.1.1 Project Sponsor Group

Dr. Paulo Costa is the sponsor for this semester's task of developing a Concept of Operations (CONOPS), Systems/Subsystem Specification (SSS), and Software Design Document (SDD) for the Air Traffic Controller Cyber Attack Evaluation Serious Game (ACES). A former fighter pilot in the Brazilian Air Force he is personally familiar with the domain and stakeholders of the proposed Serious Game. Dr. Costa is an Associate Professor at the George Mason University (GMU) Department of Systems Engineering and Operations Research and a Research Director of International C2 Activities at the GMU Command, Control, Communications, Computing, and Intelligence (C4I) Center.

1.1.2 SGI Team

The SGI team consisted of four members. Below is a brief introduction to the members and their skillsets:

- **JD Damici** is an undergraduate senior who's expected graduation date is May 2014. His area of expertise was visual enhancements and artistic design such as 3D modeling within Unity.
- **Raymond Alexander** is also an undergraduate senior expecting to graduate in May 2014. His area of expertise was artistic design and visual enhancements as well.
- **Romel Ramos** is also expecting to graduate in May 2014. His area of expertise was also in artistic design and visual enhancements.
- **Chris Cerda** is a graduating senior as well. His area of expertise ranged from programming within Unity to creating artistic models for visual enhancement.

1.1.3 SEOR Team

Our team consisted of three members whose skills ranged from program management, to operations research, to architecture and design.

- **Imran Shah** (Team lead) is a graduate student pursing an Operations Research degree.
- **Will Fontan** is a graduate student pursuing a Systems Engineering degree with a focus in Program Management.
- **Doran Cavett** is a graduate student pursing a Systems Engineering degree with a focus in Architecture based Systems Integration.

2 Background

2.1 General Description

The ACES game project is aimed at addressing the Air Traffic Management (ATM) risks encountered by air traffic controllers when challenged by a cyber-attack. It began as one of several potential GMU SE/OR capstone course research projects offered, aimed at putting learned OR/SE skills into practice.

Dr. Costa provided the initial description of the operational need to be addressed. The operational needs established by his presentation, "Simulation-based Evaluation of the Impact of Cyber Actions on the Operational C2 Domain", set the foundation for the ACES game project.

2.2 Mission

Unlike traditional games, serious games have an explicit and carefully thought-out educational purpose and are not intended primarily for amusement. Serious games can also be used to gain insights into the simulated operations and develop future planning based on what was learned ACES will provide a simulation of a real world situation and shall offer new experiences, insights, and knowledge to ATCs and observers, transforming learning into a more-engaging and dynamic process. Gameplay elements such as scoring and winning or losing are included to gauge a participant's progress with regards to established learning goals or objectives.

The operational concept described in this document is focused on cyber-attacks on helicopter operations in support of Maritime Oil Fields off the coast of Brazil. These offshore flights are often conducted at low altitudes and at distances beyond the range of any available mainland radar.

As a result, the safe and effective management of these offshore helicopter operations is then provided through the Automatic Dependent Surveillance-Broadcast (ADS-B) system.

ADS-B consists of two services ADS-B In and ADS-B Out. ADS-B allows for aircrafts and ground stations to receive ADS-B messages, air traffic messages, weather and terrain messages, ADS-B Out allows for aircraft to broadcast their identity, position, altitude, and speed to other aircraft and ground control stations. Aircrafts obtain their location from Global Positioning System (GPS) and broadcast ADS-B Out messages to other aircraft and relay or ground stations.

ADS-B communication is unencrypted and unauthenticated; anyone can listen to it and decode the transmissions from aircraft in real time. It does not make use of data level authentication of data from aircrafts; only checksums are used to verify integrity of a submitted message. ADS-B communications can be attacked through interception of messages, jamming of transmission, and injection of messages. A general description of these types of threats is shown below:

Type:	**Interception Attack**
Name:	Aircraft Reconnaissance
Description:	Intercepts and decodes ADS-B transmissions.
Purpose:	Target specific aircraft, gain knowledge about movement of assets and build an air order of battle, often the first step of a more insidious attack.
Target:	Aircraft
Technique:	Interception of ADS-B OUT signals
Difficulty:	Low

Type:	**Jamming Attack**
Name:	Ground Station Flood Denial
Description:	Disrupts the 1090MHz frequency at the ground station
Purpose:	Blocks all ADS-B signals intended for the ground station. Impact is localized to a small area determined by the range and proximity of the jamming signal to the ground station.
Target:	Aircraft and Air Traffic Controllers
Technique:	Jamming signal capable of disrupting the 1090MHz frequency range or GPS frequency
Difficulty:	Low

Type:	**Jamming Attack**
Name:	Aircraft Flood Denial
Description:	Disrupts the 1090MHz frequency for an aircraft
Purpose:	Blocks all ADS-B signals intended for an aircraft. Most significant impact involving this attack stems from gaining close proximity to an airport and affecting landing or taxi operations.
Target:	Aircraft
Technique:	Jamming signal capable of disrupting 1090MHz
Difficulty:	Medium

Type:	**Injection Attack**

Name: Ground Station Target Ghost Inject
Description: Injects an ADS-B signal into a ground station
Purpose: Cause illegitimate (i.e., ghost) aircraft to appear on the ground controller's console.
Target: Ground Station
Technique: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic.
Difficulty: Medium-High

Type: **Injection Attack**
Name: Aircraft Target Ghost Inject
Description: Injects an ADS-B signal into an aircraft
Purpose: Cause illegitimate (i.e., ghost) aircraft to appear on an aircraft's console.
Target: Aircraft
Technique: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic
Difficulty: Medium-High

Type: **Injection Attack**
Name: Ground Station Multiple Ghost Inject
Description: Injects ADS-B signals into a ground station
Purpose: Overwhelm the surveillance system and create mass confusion for the ground controller
Target: Ground Station
Technique: Inject multiple messages that conform to ADS-B message protocol and mirrors legitimate traffic
Difficulty: Medium-High

Current ABS-B vulnerabilities and their possible exploitation are of interest to a wider audience due to mandatory use of ADS-B in the United States by 2020 and in Europe by 2017. ADS-B is already in use in parts of North America, Europe, China, and Australia.

2.3 Operations

The operational setting for the ACES game is Brazil's Campos Basin where over 30 oil fields managed by large corporations such as, Petrobras, Esso, and Shell, are located. The Campos Basin region accounts for over 1 million barrels a day of petroleum production (80% of Brazil's petroleum production). Oil development operations in the Campos Basin include heavy helicopter traffic between the continent and oceanic fields during daytime, with an average of 50 minutes per flight.

Figure 1- Overview of Campos Basin Oil Operations

Helicopter flights are conducted at low altitudes and oil platforms are located more than 60 nautical miles from the region's main airport, Macaé. As a result, helicopter operations cannot be monitored from the Macaé airport, the region's main airport, which only supports air traffic within a 45 nautical mile radius and 9500 foot and above altitude. ATM for these offshore helicopter operations is then provided through the ADS-B system.

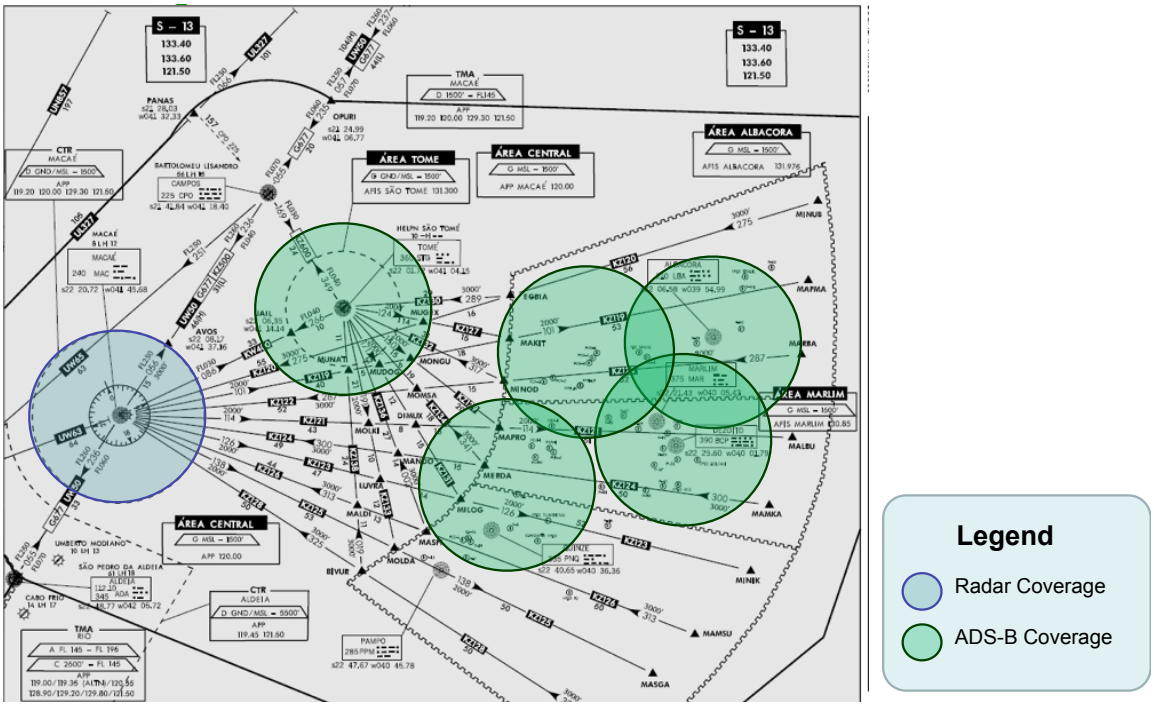


Figure 2 - Campos Basin Radar & ADS-B Coverage

2.4 Problem Statement

Disruption to the Campos Basin helicopter operations will negatively impact and may even halt production at the oceanic fields. Safe and continuous operation of helicopters supporting offshore oil production is critical to meet production capabilities and protect against loss of life or assets.

ATC reliance on ADS-B may allow for hostile individuals to disrupt helicopter operations through various cyber-attacks. There is no current means to train ATCs to detect and react to cyber attacks against ADS-B communication. There is also a need for the means to better understand the potential mission impacts of cyber threats and to allow for the development of improved operational and risk management processes for helicopter operations in the Campos Basin Region.

3 Scope

3.1 Objectives

The objective of this semester's work is to develop a CONOPS, SSS, and SDD for a serious game that will model cyber attacks against helicopter operations in support of oil development in the Campos Basin region of Brazil.

The game will allow ATC players to detect and react to ADS-B cyber attacks and allow for analysis of impact to oil development operations as a result of ADS-B cyber attacks.

3.2 Technical Approach

Unlike traditional games, serious games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. A serious game provides simulation of a real world situation and offers new experiences, insights, and knowledge to game players and observers, transforming learning into a more-engaging and dynamic process. Gameplay elements such as scoring, the possibility of winning or losing and embedded prizes may also be included to gauge a participant's progress with regards to established learning goals or objectives.

As described above, ADS-B cyber-attacks can focus on either aircrafts or ground stations. We will develop requirements and a Concept of Operations (CONOPS), requirements, and a series of software design guidelines for a serious game that simulates the effect of cyber attacks on helicopter operations in support of Maritime Oil Fields off the coast of Brazil. The scenario will model Air Traffic Control operations in the Campos Basin and serve as a training tool for Air Traffic Controllers to help detect and respond to ADS-B cyber attacks.

This problem was new for each individual on the SEOR and the SGI teams and because of that we deployed the use of a spiral development cycle to gain a better understanding of the technologies, scope our problem down to a manageable piece, and for learning one another's skills. When the project began we were given an overview of the problem presented by Dr. Costa, which detailed out the scenario in Brazil and some of the work that Dr. Barreto had previously completed. After the introduction to the SGI team and wrapping our heads out the problem space we start to determine a best way forward for integrating in with the SGI group as well as provide our Sponsor a product by the end of the semester that added value to the C4I Center and could help future groups continue the work. Below in Figure 3 you will see the spirals that our group went through in working towards our final recommendations and solutions for the semester.

We as a team would meet on a weekly basis with the SGI group to share progress on our respective ends and to have an open forum for problem or issues that anyone was having. We provided guidance for the SGI team as to what the game should look like, how RADAR works, what ADS-B technology was, general knowledge about helicopters and their characteristics. The teams had to share a fair amount of knowledge with one another to better understand each others goals since this was not a project to satisfy one teams needs, it was to serve as a final project for both the SGI group as well as the SEOR. This is what ultimately led our group to settling on doing a proof of concept design inside of Unity after we could not get VR-Forces and Unity to integrate together in the manner that we had originally hoped. The SGI team needed

to produce a product for their design class and we wanted to show the powers and capabilities of Unity.

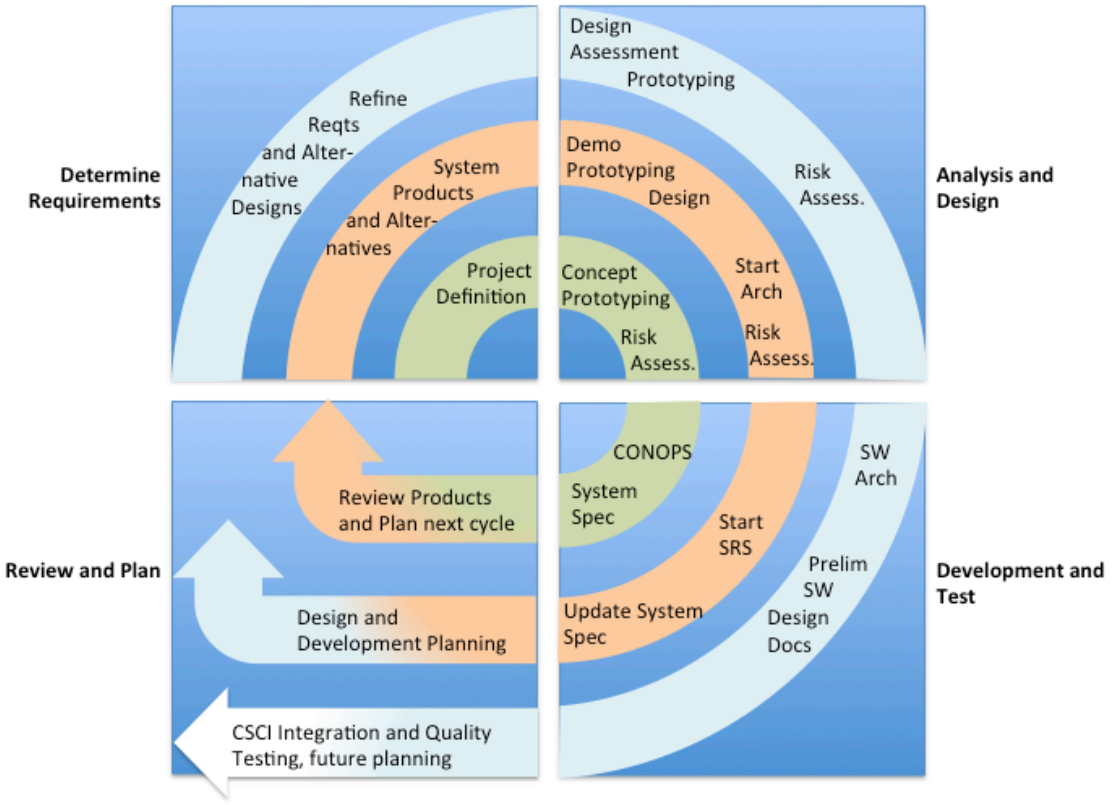


Figure 3 - ACES Spiral Development Model

Key parameters or capabilities ACES should take into consideration for scoring/metrics purpose are shown in table 1 below. The first three capabilities are indicative of Computer, Communication, and Information concerns, risks, and/or issues ATM personnel would be confronted with, which the last three are of grave Command and Control interest.

Capability	Attribute	Measure	Metric
Attack Detected and Positively Identified	Attack Characteristics and Pattern	Attack Type, Target, and Technique	Volume detected; % detected; % positively identified
Identified attacks quarantined[2]	Number of Affected Devices and Response Time	Number of consoles quarantined and recovered	% of ATC consoles recovered; Time of recovery[1]

Capability	Attribute	Measure	Metric
Recovery to Attack Event	Computer Terminal Down Time	Time to full recovery from attack	Time to recovery
Mission Assurance	Flight operations to and from Oil Platforms	Operations Tempo (OPTEMPO)	Sortie Generation Rate; Average mission fuel consumption; Average mission flight time
Mission Assurance	Flight operations to and from Oil Platforms	Mission Reliability (MR)	% of flight operations successfully completed
Schedule Adherence	Late Flight Departures and Arrivals	Schedule Slippage	% of late departures & arrivals; average late departure and arrival times

Table 1 - Key Metrics

NOTES:

1. Recovery is defined as the threat has been detected, positively identified, and prescribed recovery procedures have been implemented.
2. Quarantined is defined as the cyber threat has been removed from the ATC's console.
3. Mission Reliability is defined as the probability of completing entire sortie without failure of any Mission Essential Function

The ultimate goal is to achieve some or all of the following desired technical and operational capabilities:

3.2.1 Technical

An integrated ATM cyber network defense toolset complementing existing enterprise support environments providing improved visualization, management, and protection of computer networks installed and tested at Air Towers utilizing ADS-B technologies with capabilities consisting of

- Behavior-based attack detection, counter-attack and inoculation of ATC workstations
- Leak detection of both insider and outsider threats

- Network attack data collection, data analyzed and future attack predictors
- Network operational control at Airport Tower with visibility at higher Headquarters.

3.2.2 Operational

- Means to develop and evaluate innovate CONOPS and Tactics Techniques & Procedures (TTPs) based on regression and statistical analysis from games played and from lessons learned during technical and operational demonstration events germane to new ATM technologies.
- Able to define and describe the ability of cyber network operations capabilities to support Regional and National ATM requirements.
- Means to develop to-be CONOPs and TTPs based on ongoing Research, Development, and Acquisition efforts.

3.2.3 Benefits

3.2.3.1 Reuse

Our proposed design leverages existing simulation code of helicopter operations developed for Dr. Barreto's PhD thesis and allows for building upon the code for enhancements. The team had discussions with Dr. Barreto throughout the semester and since our team lacked some of the programming experience that he possessed he was willing to work with the team to expand his code base. Though the pieces were in place the team unfortunately ran out of time in order for Dr. Barreto to implement the enhancements to his attack generator.

3.2.3.2 Accuracy

The simulation tool chosen for use, VR-Forces, allows for simulation of helicopter flights that will accurately model interactions with assets and impact to operations. The use of VR-Forces enhances the accuracy of the game scoring and analysis of impact on helicopter operations.

3.2.3.3 Realism

The use of Unity game engine for game design and 3D gameplay provides a realistic environment that allows a player to learn in a setting that closely mimics the ATC experience. Using Unity also allows for a much better integration of the SGI and SEOR team. While the SGI team can work to visually enhance the game the SEOR team can work to integrate components, define new capabilities and enhancements, and researching more information about future/current cyber-attack methods. Making the game more realistic through Unity will also help players become more immersed in the gameplay hopefully leading to better retention of knowledge rates as well as translatable skills between the serious game and the real world.

3.2.3.4 Training

Through use of data storage the player will be able to continue to play and improve score and learning over time. Statistical and trend analysis tools would be available to assist players and

supervisors to determine learning progress, as well as, the effectiveness of ACES as a learning tool.

3.2.3.5 Leveraging

Unity is a tool that is widely used by the video game development community while MAK's VR-Forces is a powerful simulation engine that can be visual enhanced by importing 3D models created within Unity. Future ACES development and prototyping teams could benefit from clear designation and scoping of work that will be performed in Unity and VR-Forces'. With our effort, both teams had to learn the capabilities of VR-Forces and most likely future teams will have to do the same. The SGI group knew Unity very well and working within it did not present as much of a learning curve for development.

3.2.4 Assumptions

3.2.4.1 General Assumptions

This project was executed under a number of assumptions. These assumptions provide boundaries and guidance necessary for the development of ACES and to be able to scope out the level of effort required by the SEOR and SGI teams.

We assume the first version of ACES will be made available at the GMU C4I Center and SGI Development Center. Initially, the user (also known as the "player") will launch ACES game from a designated workstation.

We also assume the SGI team and members of the C4I Center will provide technical support, as needed. GMU's Department of Systems Engineering and Operations Research, along with its Simulation & Game Institute will provide logistical guidance and assistance, as required.

3.2.4.2 Policy Assumptions

GMU's SGI-promulgated standards, policies and best practices pertinent to serious game development will apply in this project. Best practices fostered by the U.S. Entertainment Software Association should also be taken into consideration while developing and refining ACES. Examples of policies and best practices to be adopted are those relating to Anti-piracy, intellectual property, and parental control.

The Entertainment Software Rating Board (ESRB) rating for ACES should be ADULT (content suitable only for adults ages 18 and above) as it is comparable to the typical demographics of an ATC plus, it might include prolonged scenes of violence and/or strong language.

3.2.4.3 Licensing

Unity and VR Forces licenses will be available for future development of ACES.

3.2.4.4 Domain Knowledge

ACES game users will have appropriate knowledge to configure realistic ADS-B cyber attacks.

3.2.4.5 Operator Experience/Training

The ACES team made the assumption that users of the game would have an ATC knowledge base provided through the Federal Aviation Administration or a similar entity. With that base knowledge even new players to ACES would understand the structure of the information on the RADAR display and they would understand tracking aircraft with RADAR technology. Moving forward with this assumption will allow the ACES team and future teams to focus their efforts on the "gamification" piece of the project and not building tutorials and how-to guides to introduce players to air traffic control basics.

3.2.4.6 Helicopter Issues/Downtime

The ACES team will move forward with the assumption that helicopters being used in the serious game will not experience any type of mechanical failures while in flight. This will allow a player to focus on learning identification of issues of aircraft on their display. Though in real life a number of scenarios could arise, ranging from mechanical failure to cyber-attacks, the purpose of this game is to train controllers to notice anomalies on RADAR displays and take corrective action if a cyber-attack were to occur.

3.2.5 Risks

3.2.5.1 Support

Continued support for all COTS tools from the vendors will be available especially for VR-Link, which is required to allow Unity to interact with VR-Forces. Support is also required for development of the Attack Generation Code. Any projected shortfalls in vendor technical support cold impact ACES schedule, quality, and the robustness of available features.

3.2.5.2 Skillset

Design and development of ACES is significantly dependent on a team with skillsets in the following tools and languages:

- VR-Forces: Familiarity with the VR-Forces tool, configuring and manipulating simulations
- Unity: Familiarity with designing and manipulating a game in Unity
- C#/C++/Programming Languages: Programming skills are required for maintenance and update of attack generation code and manipulation of behaviors in Unity beyond built in actions

ATM subject matter expertise will be foreseeably required for future ACES development efforts. The entire ACES validation effort will depend on early involvement and timely feedback.

Should the team lack such skills and necessary expertise they will run the risk of facing possible schedule slips which could result in developing a product of limited, poor, or unrealistic simulation and gaming qualities.

3.2.5.3 Attack Generation Code

Attacks generated by ACES must be realistic to provide for meaningful training and analysis of impact to critical infrastructure and helicopter operations. Otherwise it may lead to erroneous simulated mission impact, along with a false sense of accomplishments by those playing ACES.

4 Model and Architecture

ACES functionality is organized into five major subsystems as depicted below:

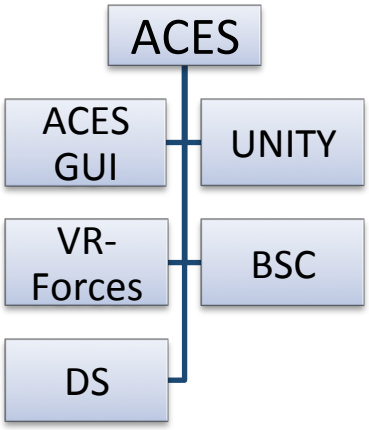


Figure 4 - ACES High Level Entities

4.1 Subsystem Descriptions

4.1.1 ACES GUI

The ACES GUI Subsystem is responsible for providing a means for users to interact with the serious game. Every aspect of the game will need a GUI in order for a user to progress or influence the gameplay. The Simulation and Gaming Institute partners as well as the C4I Center at GMU are the major stakeholders of this subsystem.

4.1.2 Unity

Unity is a COTS game development engine, fully integrated with a complete set of intuitive tools and rapid workflows to create interactive 3D and 2D content.

Unity will be used to enhance the visual aspects of ACES, such as terrain and building structures inside of the game. VR-Forces interfaces with Unity in order to accept 3-dimensional (3D)

model updates to the Geographical Information System (GIS) data that comes preloaded with the tool.

Once built, these enhanced 3D models inside of Unity will be integrated to VR-Forces and mapped to object instances so that the visual aspects of the game are appealing to the user.

For this semester the proof of concept was developed purely in Unity because of issues that were encountered

4.1.3 VR-Forces

The VR-Forces simulation subsystem was used in previous iterations of the project to perform an Operations analysis on the flight paths of the helicopters and the amount of throughput they could perform. For purposes of the serious game the intent was to utilize the previously performed work and enhance it by turning it into a serious game.

VR-Forces is a Computer Generated Forces (CGF) application and toolkit. It provides an application with a Graphical User Interface (GUI) that displays a simulated environment. Users can create simulations using pre-defined or custom entities. VR-Forces and the simulations generated can be combined with other software to develop applications and configured for access through a separate interface. VR-Forces consists of a GUI and a backend simulation engine. Each is a separate application that communicates with each other through the use of a network.

To build the ACES game prototype the SE/OR-SGI team shall leverage work previous completed in a joint effort between the GMU C4I Center and the Technological Institute of Aeronautics in Brazil.

The code that will be reused in ACES is a C++ simulation of helicopter operations in the Campos Basin region developed by Dr. Alexandre Barreto in the Fall of 2013. The C++ simulation code is run as a simulation scenario in the MAK VR-Forces simulation tool.

4.1.4 Attack Generation Code (Barreto Simulation Code - BSC)

The Cyber-Attack Simulation Subsystem is designed to be extensible for the incorporation of new attack types beyond the work performed in the Spring 2014 semester. The Cyber-Attack Simulation will interface with the Unity game environment as well as VR-Forces to simulate the attacks that it constructs and sends over for placement into the serious game.

4.1.5 Data Storage

The ACES Data Storage Subsystem consists of two components; the Database for storage and quick recall of user profile information and the Data Store that contains the functionality to write game save information to a client machine.

4.2 Architecture (Inputs/Outputs)

The figure below shows how the ACES GUI, Unity, MAK VR-Forces, Attack Generation code, and the data storage interact and share data.

The ACES GUI displays GIS data mapped to 3D entities and GIS data to the end user's display. Account data is also displayed via the GUI. Users input commands to manipulate the game (i.e. detect and respond to cyber attacks) and login/account data.

The Unity game receives GIS data from MAK VR-Forces simulation and user account data from the data storage. GIS data mapped to 3D entities is then displayed to end users via Unity.

MAK VR-Forces is responsible for conducting simulation of helicopter operations. Cyber attacks against ADS-B communication are fed into the simulation from the attack generation code and scripts stored in the data storage. MAK VR-Forces stores and retrieves simulation data by means of the data storage. GIS data is sent to Unity for eventual display to end-users. End user commands are able to modify execution of the simulation.

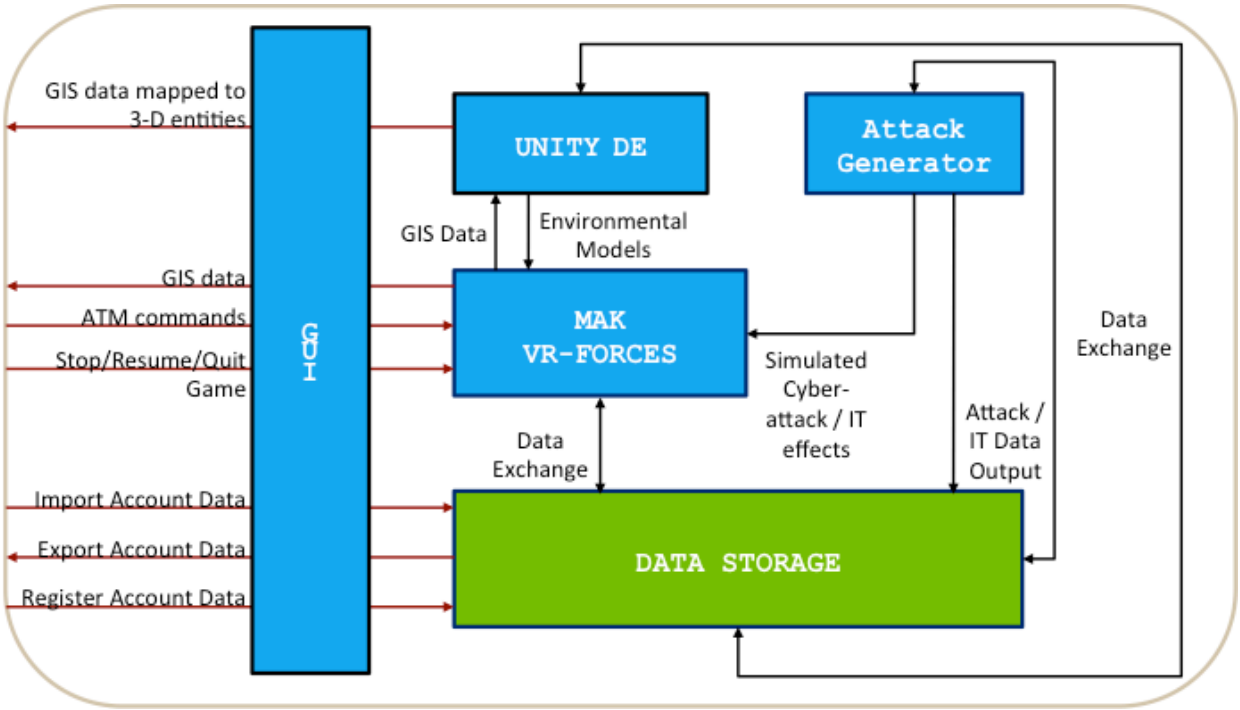


Figure 5 - ACES Interactions

4.3 ACES State Transition Diagram

The state transition diagram below shows the transitions between the states for the ACES. This diagram summarizes how the ACES game moves from one state or mode to another.

The beginning state is the LAUNCH state where the player logs in or creates a new account. For new players, the system goes into the INITIATION state, which is where the GUI menu is present for entering new player's information and offers a USER CHECK. This check will consist of various tutorials and general description segments of ACES' components or elements.

After initialization (or after the LAUNCH state for returning players), the ACES game transits to an OPENING SEQUENCE state, where the player eventually chooses the game's level of difficulty and initiates a game session.

Prior to, during, and after a game session, the player can go to the USER CHECK state to revisit the tutorial and/or general description segments. If the game is in session, ACES will have to go through the PAUSE state before entering to any other state.

When the ACES game session is completed (or paused), ACES can transition to the END GAME state, the USER Check state (as described above), or back to the OPENING SEQUENCE state (to initiate another game session). Whenever a game session is completed, ACES will momentarily transition into a SUMMARY state to reflect the player's scores and progress.

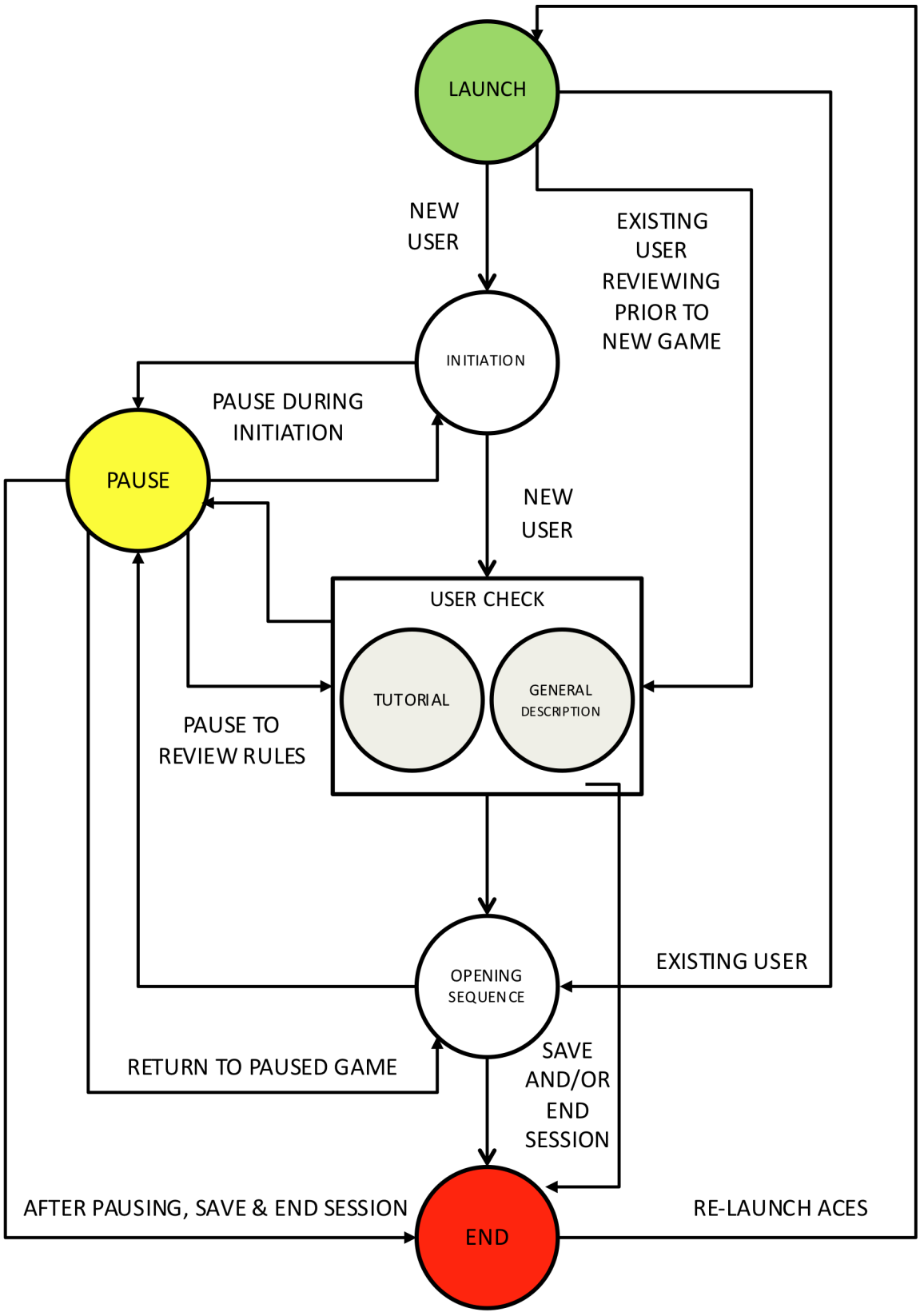


Figure 6 - ACES State Transition Diagram

4.4 Concept of Operations

The ACES game CONOPS describes at a high level how the ACES game will be employed to mitigate the impact of a cyber-attack to an ADS-B based ATM system. Storyboards were used to assist in the developments of the ACES concept of operations due to the program's highly demanding schedule. They provided a timely iterative development process between the SEOR team, the SGI team, the Sponsors, and Professors. Ensuing requirement documents include the traditional use cases for the design and development teams to go by. The CONOPS also help s codify future ADS-B based ATM cyber-security design and development decisions.

The following storyboards are documented in the ACES CONOPS:

- SB 1: Creating New Account and ACES Tutorial
- SB 2: Launching ACES
- SB 3: ACES Cyber-Attack Injects
- SB 4: ACES General Description & Normal Operational Tempo Guidance
- SB-5. ACES Scoring / Point / Rewards System
- SB-6. Ghost Track Behavior
- SB-7. ACES Levels of Difficulty
- SB-8. Capturing Lessons Learned / Trend analysis
- SB-9. ACES Graphical User Interface

4.5 System/Subsystem Specification

This SSS describes the requirements for ACES. The SSS serves as the complete set of requirements necessary for ACES to continue into future stages of development. This SSS contains all the requirements necessary to design and build the ACES in full compliance with the requirements and expectations of the SEOR Team. Along with requirements for ACES and its subcomponents the SSS contains use cases for the following scenarios:

- Launching ACES
- Account Initiation
- Utilizing User Check
- The Opening Sequence and Starting a Game Session
- Pausing and Resuming a Game
- MENU Options: Saving and Quitting a Game
- MENU Options: Accessing Help & Utilities Tools
- MENU Options: Accessing Statistics and Scores

4.6 Software Design Document

The SDD is a standalone document that describes the architecture of ACES. The document covers how to integrate Commercial Off the Shelf (COTS) software components that make up the ACES game beginning with the integration of VR-Forces simulation tool and the Unity game engine.

5 Validation

Project validation was primarily achieved by periodically interacting with our sponsor, Dr. Paulo Costa – Research Director for International Command and Control activities at the George Mason University's C4I Center – throughout the entire semester. First, a kick-off teleconference was held with Dr. Paulo Costa (C4I Center) early in the semester to review the C4I Center's needs and expectations. Dr. Costa provided the SEOR team and overview of the research completed by LtCol Barreto into evaluating the effect of cyber attacks on critical infrastructure. The SEOR team then digested the information and internally discussed the task and various approaches to developing a CONOPS and requirements for a serious game that evaluates cyber attacks against critical infrastructure.

Soon thereafter, the SEOR team met with Dr. Costa and the SGI team to convey the sponsor's needs, along with their immediate interpretation of the scope of work, suggested approach of serious game to train ATCs to detect and respond to ADS-B cyber attacks, and to begin formalizing general roles and responsibilities amongst both teams. Following Dr. Costa's approval of the proposed game the SEOR team began development of high level requirements to guide the SGI team in development of a rapid prototype.

The team initially desired to guide the SGI team in development of an ACES prototype that included all of the subsystems identified in section 4.1. However due to difficulties encountered in integrating the simulation engine VR-Forces with the gaming engine Unity a modified set of objectives was created for this semester. The SEOR team continued to work towards development of a CONOPS and system / subsystem requirements document for the desired serious game in is end state. A Software Design Document was also added to help guide future teams working on ACES to understand the design decision made and guide integration of COTS tools required for the serious game. The SGI team focused on delivery of a proof of concept game for ACES developed purely in the Unity game engine. The modifications to deliverables were presented to and approved by all sponsors and stakeholders.

On a weekly basis a joint SEOR-SGI team meeting was held to discuss risks, activities completed, assignments for the next week, and action items. Meeting minutes were documented and distributed to stakeholders and the project sponsor within 12 hours of each meeting. Meeting minutes were used as a communications channel to verify all stakeholders agreed on the state

and direction of the project. Weekly meeting minutes were also used to trigger communication between parties in the form of discussions or questions that arose based on the interaction documented.

Several ad hoc project updates were given to Dr. Costa throughout the semester. Feedback received from him was then considered in a timely fashion, shared with project stakeholders, and then used to adjust the project's goals and objectives accordingly. Finally, Dr. Costa conducted a critical documentation review in late April and all planned deliverables were revised before being tendered.

Project validation was also achieved through other stakeholders namely, the SGI team and Dr. Laskey, the SYST/OR 699 professor. Weekly teleconferences and periodic project reviews gave ample opportunities for the SOER team to fine-tune their deliverables, in particular, their proposed way forward. All stakeholders reviewed all draft deliverables and their feedback was taken into consideration, along with Dr. Costa's.

Research and findings identified concerning the integration of Mak VR-Forces and Unity were reviewed and discussed with representatives and developers from Mak to verify the appropriateness of our recommendations. A series of technical discussions occurred between the SEOR team and the technical support team at MAK, the developers of the VR-Forces product. As one of the software products we were asked to utilize, the deliberations that took place proved to be critical for shaping the resulting proof of concept and more importantly, the proposed way forward.

6 Issues

6.1 Background Knowledge and Tool Expertise

Neither the SEOR nor the SGI team possessed expertise in VR-Forces or the C++ simulation code developed by LtCol Barreto. A training session was held early in the semester to acclimate both teams to the VR-Forces software. Unfortunately integration with Unity was not covered in technical detail resulting in delays in project execution.

In addition the C++ simulation code developed by LtCol Barreto did not have any supporting documentation and wasn't able to be modified or utilized this semester as a result.

6.2 Integration of Unity and VR-Forces

VR-Forces entities are not capable of direct manipulation from Unity. The SDD describes the steps required to integrate VR-Forces and Unity.

6.3 Coordination of Efforts and SEOR Team Oversight

Due to the time required for "ramp up" and learning of the ACES software the SEOR team was not able to provide direction for game design early in the semester. A set of high level requirements were provided to serve as a guide for the SGI team's development of a proof of concept which resulted in a less than robust proof of concept serious game. As CONOPS/SSS/SDD development and refinement occurred throughout the semester the SEOR team's oversight of SGI game development occurred as a separate unrelated task due to avoid providing the SGI team a "moving target" of requirements.

7 Findings and Recommendations

7.1 Skillset

Future teams should verify that at least one member of the SEOR and SGI groups possesses programming experience specifically C++/C#. Experience in these language is required to extend behaviors in VR-Forces and Unity. Programming expertise will also assist with update and modification of the attack generation code.

7.2 Domain Expertise

Review and input from ATCs will be helpful to refine the design and verify the gameplay is realistic and understand how the game can be improved in training an ATC.

7.3 Unity Player Interaction with VR-Forces Simulation Entities

7.3.1 VR-Forces Tasks

A task in VR-Forces can cause an entity to move to a location, patrol a route, follow an entity, take off / land, or fly to a location. VR-Forces allows for custom tasks to be written in the Lua scripting language.

7.3.2 Reactive Tasks in VR-Forces

A reactive task is only executed if a condition is met. The simulation is monitored and a reactive task is executed when a condition is fulfilled.

7.3.3 Suggested Approach

VR-Link for Unity doesn't directly allow for the manipulation of VR-Forces entities from Unity. However a task can be configured in VR-Forces that allows a VR-Forces entity to react to the behavior of another entity (the entity to which a VR-Forces entity reacts can be either in Unity of VR-Forces). In this configuration a VR-Forces entity, for example, can be configured to change directions of speed once a Unity entity enters an area or is within a certain distance of another entity. This indirect means of controlling a VR-Forces entity through Unity is suggested for implementation by future teams through a control panel interface for the ATC.

The table below captures the interactions required between VR-Forces and Unity. Limitations of VR-Link for Unity are explained along with potential workarounds.

VR-Forces and Unity Interaction				
Source	Destination	Data Exchanged	Desired Result	Feasibility
VR-Forces	Unity	Position of VR-Forces simulation entities	Display VR-Forces simulation entities in Unity game	Supported though VR-Link for Unity as described in the SDD
Unity	VR-Forces	Player interaction with VR-Forces simulation entities	Change in movement/operation of VR-Forces simulation entities	Unsupported directly. Workarounds discussed below the table
VR-Forces	Unity	Scoring: Landing of helicopters / Near accidents / Violation of helicopter operation rules (too high, too low, too close to others)	Provide data to allow for scoring of player	Captured purely in Unity and supported though VR-Link for Unity as described in the SDD

Table 2 - VR-Forces and Unity Interaction

7.4 CONOPS

There is a wide range of risk tradeoff analysis to be taken into consideration when the user is conflicted between ensuring continuity of critical operations (Operational Risk) and safeguarding all computer and communication assets during a cyber-attack (IT Risk). At some point, the same hardware and software elements (that enables the Command and Control functions) must be preserved, often time resulting in mission degradation. At some point, the repercussions of a chosen immediate action path can be felt during the ensuing recovery efforts.

Existing and possible backup hardware and software tools will also play a significant role on how the user will play ACES (e.g. Cell phones/SATCOM). The same should apply for secondary means of gathering information during normal and critical operations (e.g. a helicopter or plane flying nearby a suspected ghost track; even a ship).

The risk attitude of the player, along with any promulgated ATM "rules of engagement" will play a significant role in shaping up the "as-is" and "to-be" tactics, techniques, and procedures (TTPs) utilized (discovered or experimented with) by the ACES players. Night and/or foul weather TTPs can be significantly different that those during daytime/fair weather conditions. A subtle cyber-attack might be very difficult to detect during adverse weather condition and to mitigate such risks, additional preventive measures (either procedurally or through software/hardware schemes) could be added.

To summarize, a deeper look into these tradeoff spaces is in order, should this effort be continued by future SEOR graduate teams. Although very time consuming, the creation of a user integrated product team and/or the use of interviews / questionnaires / surveys to solicit vital information from the ATC community and other ATM subject matter experts would be prudent.

8 Future Work

The following game improvements can be made:

- Display Barreto Simulation of helicopter operations in the Unity designed game
  - The existing proof of concept displays hard coded aircrafts. Integration of LtCol Barreto's code will facilitate realistic aircraft simulation.
- Implement suggested method for influencing VR-Forces entities from Unity.
  - Integration of VR-Forces with Unity will allow for end users to enjoy a gaming experience while interacting with a robust simulation of helicopter operations in the Campos Basin region.
- Develop game point/win-lose methodology and learning trend analysis tool
  - Scoring and trend analysis will allow for tracking of an ATC's progress.

The following additions to a ATM Cyber Network Defense Toolset can be made:

- Develop behavior-based attack detection, counter-attack, and inoculation of ATC workstations tools
  - Looking beyond training automated detection and response recommendations will help assist an ATC in his/her job.
- Develop Network attack data collection, data analysis, and future attack prediction tools
  - Analysis of valid ADS-B compared to injected messages will allow for development of prediction tools.
- Develop Future Operational Concept and Tactics Techniques & Procedures (TTPs) to evaluate with ACES
  - Input from subject matter experts will assist in the development of these TTPs.

The following programmatic and technical approaches should be examined:

- Establish a User Integrated Product Team (IPT) to validate simulated air operations and cyber-attack injects.
- Consider implementing an agile software spiral development whenever appropriate.
    - Agile software development will allow for rapid prototype and feedback loops that allow for stakeholders to provide their suggested changes throughout the development process.
- Consider expanding list of stakeholders to include representatives from Mak VR-Forces and members of past SEOR-SGI teams.
    - Expert input and past experience will help avoid past pitfalls and obstacles.

APPENDICES

Project Management

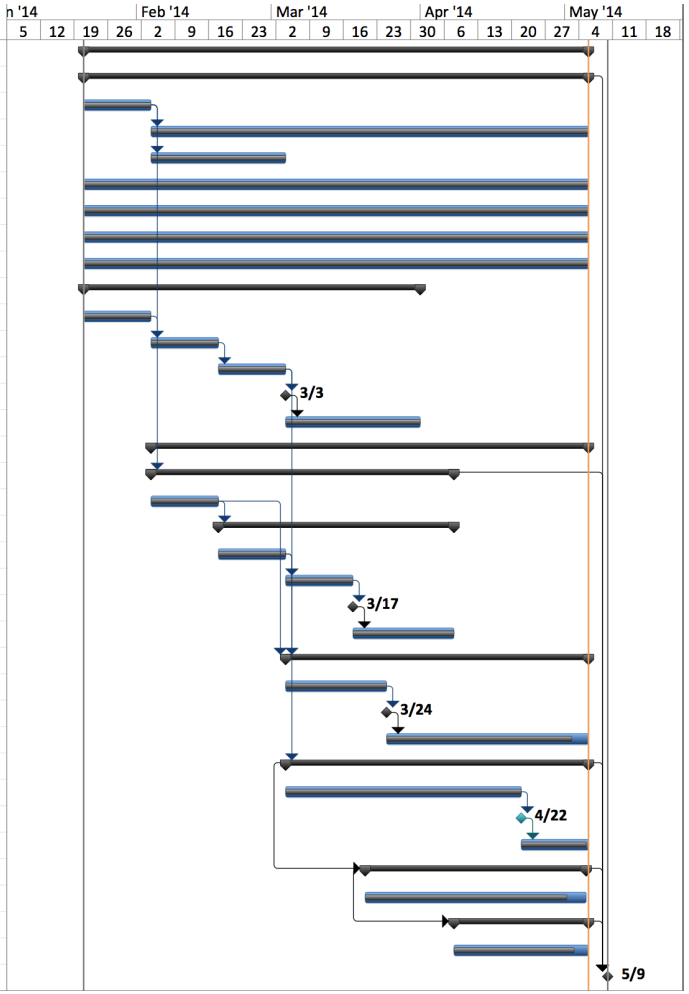
Acronym List

References

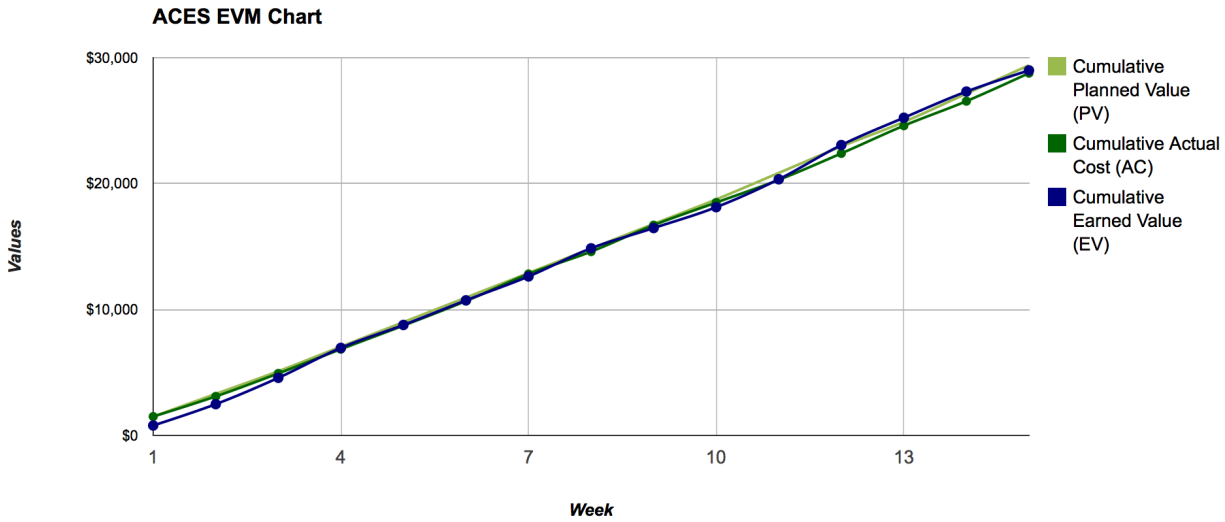
Appendix A: PROJECT MANAGEMENT

GANTT Chart

ID		% Complet	Task Name	Duration	Start
1		**99%**	**Serious Game for Cyber Threat Impact Assessment**	**75 days**	**Tue 1/21/14**
2	✓	**100%**	**PROJECT MANAGEMENT**	**75 days**	**Tue 1/21/14**
3	✓	100%	Staffing	2 wks	Tue 1/21/14
4	✓	100%	Stakeholder Engagement	13 wks	Tue 2/4/14
5	✓	100%	ID and Provide SEOR/SGI Resources needs	1 mon	Tue 2/4/14
6	✓	100%	Integrated Management Schedule	15 wks	Tue 1/21/14
7	✓	100%	Earned Value Management	15 wks	Tue 1/21/14
8	✓	100%	Weekly SEOR Synch Meetings	15 wks	Tue 1/21/14
9	✓	100%	Weekly Reports to Sponsors	15 wks	Tue 1/21/14
10	✓	**100%**	**Proposal Development Phase**	**50 days**	**Tue 1/21/14**
11	✓	100%	Define Project Parameters	2 wks	Tue 1/21/14
12	✓	100%	Develop Project Concept Statement	2 wks	Tue 2/4/14
13	✓	100%	Develop Project Proposal	2 wks	Tue 2/18/14
14	✓	100%	***1_Project Proposal Submittal***	0 days	Mon 3/3/14
15	✓	100%	*Proposal Reviews & Updates*	4 wks	Tue 3/4/14
16		**97%**	**SYSTEM ENGINEERING / OPS RESEARCH**	**65 days**	**Tue 2/4/14**
17	✓	**100%**	**CONOPS & REQUIREMENTS**	**45 days**	**Tue 2/4/14**
18	✓	100%	Conduct CONOPS & REQTS Research	2 wks	Tue 2/4/14
19	✓	**100%**	**Develop Concept of Operations**	**35 days**	**Tue 2/18/14**
20	✓	100%	Define Actors, Scenarios and Use Cases	2 wks	Tue 2/18/14
21	✓	100%	Draft CONOPS Document	2 wks	Tue 3/4/14
22	✓	***100%***	***2_CONOPS Document Finalized***	***0 days***	***Mon 3/17/14***
23	✓	100%	*CONOPS Document Review & Updates*	3 wks	Tue 3/18/14
24		**97%**	**Develop Requirements & Specification Documents**	**45 days**	**Tue 3/4/14**
25	✓	100%	Develop System / Subsystem Specification (SSS) Document	3 wks	Tue 3/4/14
26	✓	100%	***3_SSS Document Finalized***	0 days	Mon 3/24/14
27		95%	*SSS Document Review & Updates*	6 wks	Tue 3/25/14
28		**99%**	**System Design Support**	**45 days**	**Tue 3/4/14**
29	✓	100%	Develop Software Design Document (SDD)	7 wks	Tue 3/4/14
30	✓	100%	***4_SDD Finalized***	0 days	Tue 4/22/14
31		95%	*SDD Review & Updates*	2 wks	Tue 4/22/14
32		**94%**	**System Development Support**	**32 days**	**Thu 3/20/14**
33		94%	Development Support to SGI Team	32 days	Thu 3/20/14
34		**95%**	**Proof of Concept Support**	**20 days**	**Tue 4/8/14**
35		95%	Proof of Concept Support	4 wks	Tue 4/8/14
36		0%	***5_Final Presentation***	1 day	Fri 5/9/14



ACES EVM Chart



Planned Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1	PROJECT MANAGEMENT	296	28	30	28	26	22	18	14	14	13	13	13	17	18	21	21
1.1	*Initiation Phase*	*61*	*12*	*14*	*12*	*10*	*7*	*4*	*1*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

Planned Hours Worksheet

	WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1.1.1	Define Project Parameters	0															
1.1.2	Develop Project Concept Statement	0															
1.1.3	Develop Project Proposal	0															
1.1.4	Proposal Reviews & Updates	2							1	1	0	0	0				
1.2	*Planning Phase*	*28*	*3*	*3*	*3*	*3*	*2*	*1*	*0*	*0*	*0*	*0*	*0*	*1*	*4*	*4*	*4*
1.2.1	Staffing	4	1	1	1	1	0	0	0	0	0	0	0	0			
1.2.2	Stakeholder Accountability	18	1	1	1	1	1	0	0	0	0	0	0	1	4	4	4
1.2.3	SEOR/SGI Resources needs	6	1	1	1	1	1	1	0	0	0	0	0	0			
1.3	Integrated Management Schedule	*15*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
1.4	Earned Value Management	*15*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*

Planned Hours Worksheet

	WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1.5	Weekly SEOR Synch Meetings	*90*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*	*6*
1.6	Weekly Reports to Sponsors	*51*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*6*	*6*
1.7	Others	*36*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*5*	*3*	*3*	*3*
2	SYSTEMS DEVELOPMENT	292	*2*	*6*	*8*	*13*	*17*	*21*	*25*	*25*	*26*	*26*	*29*	*25*	*21*	*24*	*24*
2.1	REQUIREMENTS ANALYSIS (RA)	*47.5*	*2*	*6*	*8*	*13*	*11.5*	*7*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.1.1	RA Research	47.5	2	6	8	13	11.5	7	0	0	0	0	0	0	0	0	0
2.1.2	Others	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2	DESIGN	*72.5*	*0*	*0*	*0*	*0*	*5.5*	*14*	*25*	*19*	*0*	*0*	*0*	*0*	*3*	*3*	*3*
2.3	DEVELOPMENT	*63.5*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*6*	*19.5*	*13*	*7*	*0*	*6*	*6*	*6*
2.4	TEST / SDD	*81.5*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*6.5*	*13*	*22*	*25*	*3*	*6*	*6*

Planned Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
2.5	Others	27	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*9*	*9*	*9*
	Total Planned Hours	588	30	36	36	39	39	39	39	39	39	39	42	42	39	45	45
	Cumulative Planned Hours		30	66	102	141	180	219	258	297	336	375	417	459	498	543	588

Actual Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1	PROJECT MANAGEMENT	320.5	23	25.5	29	32.5	30.5	31	25	17.5	16	14	14	13	17	15	17.5

Actual Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1.1	*Initiation Phase*	*81.5*	*14*	*10.5*	*11*	*11*	*10*	*19*	*5*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1.1.1	Define Project Parameters		6	5	3	5	4	3	2	0	0	0	0	0	0	0	0
1.1.2	Develop Project Concept Statement		4	5	7	4	3	7	0	0	0	0	0	0	0	0	0
1.1.3	Develop Project Proposal		2	0.5	1	2	3	4	0	0	0	0	0	0	0	0	0
1.1.4	Proposal Reviews & Updates		2	0	0	0	0	5	3	1	0	0	0	0	0	0	0
1.2	*Planning Phase*	*55.5*	*4*	*5.5*	*6.5*	*6.5*	*6*	*6*	*4*	*3*	*3*	*1*	*1*	*1*	*3*	*3*	*2*
1.2.1	Staffing		3	3	3	5	4	3	0	0	0	0	0	0	0	0	0
1.2.2	Stakeholder Accountability		1	1	1	1	1	2	1	1	1	0	0	0	3	3	2
1.2.3	SEOR/SGI Resources needs		0	1.5	2.5	0.5	1	1	3	2	2	1	1	1	0	0	0

Actual Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
1.3	Integrated Management Schedule	*14.5*	*0*	*0*	*2*	*0*	*0*	*0*	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*3*	*1.5*
1.4	Earned Value Management	*30*	*0*	*0*	*1*	*3*	*3*	*3*	*3*	*3*	*2*	*1.5*	*1.5*	*1.5*	*2.5*	*3*	*2*
1.5	Weekly SEOR Synch Meetings	*68*	*0*	*4.5*	*7.5*	*10*	*9.5*	*2*	*7*	*3.5*	*5*	*3.5*	*3.5*	*2.5*	*3.5*	*3*	*3*
1.6	Weekly Reports to Sponsors	*47*	*5*	*5*	*1*	*2*	*2*	*1*	*5*	*3*	*3*	*2*	*2*	*2*	*3*	*3*	*8*
1.7	Others	*24*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*3*	*2*	*5*	*5*	*5*	*3*	*0*	*1*
2	SYSTEMS DEVELOPMENT	255	*7*	6.5	7.5	6	7	8	18	18	26	22	22	29	27	24	27
2.1	REQUIREMENTS ANALYSIS (RA)	*142*	*7*	*6.5*	*7.5*	*4*	*7*	*8*	*12*	*6*	*5*	*7*	*7*	*13*	*11*	*24*	*17*
2.1.1	RA Research		7	6.5	7.5	4	7	6	11	2	3	1	1	1	1	0	1
2.1.2	Others		0	0	0	0	0	2	1	4	2	6	6	12	10	24	16

Actual Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04
2.2	DESIGN	*93*	*0*	*0*	*0*	*2*	*0*	*0*	*6*	*9*	*16*	*12*	*12*	*13*	*13*	*0*	*10*
2.3	DEVELOPMENT	*20*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*3*	*5*	*3*	*3*	*3*	*3*	*0*	*0*
2.4	TEST	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.5	Others	0	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
	Total Actual Hours	575.5	30	32	36.5	38.5	37.5	39	43	35.5	42	36	36	42	44	39	44.5
	Cumulative Actual Hours		30	62	98.5	137	174.5	213.5	256.5	292	334	370	406	448	492	531	575.5

NOTES:

1. Hourly Labor of OR/SE = $50.00 / hr

Actual Hours Worksheet

		WEEK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Element #	ACTIVITY	Total	w/e 1/26	w/e 2/2	w/e 2/9	w/e 2/16	w/e 2/23	w/e 3/2	w/e 3/9	w/e 3/16	w/e 3/23	w/e 3/30	w/e 4/6	w/e 4/13	w/e 4/20	w/e 4/27	w/e 5/04

2. AC = Actual Cost

3. Use this worksheet to help calculate the Actual Cost (AC) of Work Performed (ACWP) by entering the costs incurred each period.

4. Transfer the Cumulative Actual Cost to the Report worksheet.

Earned Value Worksheet

Cumulative Earned Value (EV)

WBS	Task Name	TBC	Wk 1	Wk 2	Wk 3	Wk 4	Wk 5	Wk 6	Wk 7	Wk 8	Wk 9	Wk 10	Wk 11	Wk 12	Wk 13	Wk 14	Wk 15
1	PROJECT MANAGEMENT	$14,800.00	5%	14%	27%	39%	49%	56%	63%	69%	76%	82%	89%	94%	96%	99%	100%
1.1	*Initiation Phase*	$3,050.00	4.50 %	18.75 %	47.00 %	75.50 %	92.00 %	99.75%	99.80%	99.90%	100.00 %	100.00%	100.00 %	100.00 %	100.00 %	100.00 %	100.00 %
1.1.1	Define Project Parameters	$0.00	10%	25%	60%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Earned Value Worksheet

Cumulative Earned Value (EV)

WBS	Task Name	TBC	Wk 1	Wk 2	Wk 3	Wk 4	Wk 5	Wk 6	Wk 7	Wk 8	Wk 9	Wk 10	Wk 11	Wk 12	Wk 13	Wk 14	Wk 15
1.1.2	Develop Project Concept Statement	$0.00	5%	20%	50%	75%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
1.1.3	Develop Project Proposal	$0.00	0%	15%	40%	60%	80%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
1.1.4	Proposal Reviews & Updates	$100.00	0%	0%	0%	40%	80%	95%	96%	98%	100%	100%	100%	100%	100%	100%	100%
1.2	*Planning Phase*	$1,400.00	4%	9%	27%	41%	50%	57%	63%	69%	75%	81%	86%	91%	95%	97%	100%
1.2.1	Staffing	$200.00	25%	25%	75%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
1.2.2	Stakeholder Accountability	$900.00	0%	8%	17%	25%	33%	42%	50%	58%	66%	74%	82%	88%	92%	96%	100%
1.2.3	SEOR/SGI Resources needs	$300.00	0%	0%	25%	50%	68%	72%	76%	80%	84%	88%	90%	95%	100%	100%	100%
1.3	Integrated Management Schedule	$750.00	0%	10%	20%	31%	38%	45%	54%	63%	70%	77%	86%	93%	97%	100%	100%
1.4	Earned Value Management	$750.00	0%	10%	18%	25%	32%	40%	50%	59%	70%	78%	86%	93%	97%	100%	100%

Earned Value Worksheet

Cumulative Earned Value (EV)

WBS	Task Name	TBC	Wk 1	Wk 2	Wk 3	Wk 4	Wk 5	Wk 6	Wk 7	Wk 8	Wk 9	Wk 10	Wk 11	Wk 12	Wk 13	Wk 14	Wk 15
1.5	Weekly SEOR Synch Meetings	$4,500.00	7%	15%	22%	30%	37%	45%	54%	62%	70%	78%	86%	93%	95%	98%	100%
1.6	Weekly Reports to Sponsors	$2,550.00	7%	15%	22%	30%	37%	45%	54%	62%	70%	78%	86%	93%	95%	98%	100%
1.7	Others	$1,800.00	6%	12%	18%	24%	30%	36%	43%	53%	62%	73%	84%	90%	95%	100%	100%
2	SYSTEMS DEVELOPMENT	$14,600.00	0%	2%	4%	8%	11%	17%	23%	32%	36%	41%	49%	63%	75%	87%	97%
2.1	REQUIREMENTS DEV	$2,375.00	0%	15%	26%	47%	60%	72%	81%	89%	91%	93%	94%	96%	97%	99%	100%
2.1.1	Research & Analysis	$2,018.75	0%	18%	30%	55%	70%	85%	95%	98%	99%	100%	100%	100%	100%	100%	100%
2.1.2	Documentation	$356.25	0%	0%	0%	0%	0%	0%	0%	35%	44%	54%	63%	73%	82%	90%	97%
2.2	DESIGN	$3,625.00	0%	0%	0%	0%	5%	20%	35%	43%	51%	60%	68%	80%	89%	97%	100%
2.3	DEVELOPMENT	$3,175.00	0%	0%	0%	0%	0%	0%	5%	30%	40%	50%	60%	70%	80%	85%	94%
2.4	PROOF OF CONCEPT SPPT	$4,075.00	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	15%	35%	55%	75%	95%
2.5	Others	$1,350.00	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	50%	80%	100%

Earned Value Worksheet

Cumulative Earned Value (EV)

WBS	Task Name	TBC	Wk 1	Wk 2	Wk 3	Wk 4	Wk 5	Wk 6	Wk 7	Wk 8	Wk 9	Wk 10	Wk 11	Wk 12	Wk 13	Wk 14	Wk 15
		Cumulative EV	$789	$2,484	$4,574	$6,955	$8,778	$10,732	$12,628	$14,863	$16,471	$18,129	$20,347	$23,064	$25,234	$27,314	$28,995

NOTES:

1. This worksheet is used to help calculate the Earned Value (EV) or Budgeted Cost of Work Performed (BCWP).

2. Make sure that the WBS, Task Name, and TBC are identical to the table in the Report worksheet.

3. Enter the % Complete for each task to calculate the cumulative earned value.

Appendix B: ACRONYM LIST

ACES	Air Traffic Controller Cyber Attack Evaluation Serious (Game)
ATC	Air Traffic Controller
ATM	Air Traffic Management
C4I	Command, Control, Communications, Computer, and Information
GMU	George Mason University
HW	Hardware
HELO	Helicopter
IA	Information Assurance
OA	Operational Assessment
OILPLAT	Oil Platform
OR	Operations Research
SE	Systems Engineering
SEOR	Systems Engineering and Operations Research
SGI	Simulation and Gaming Institute
SME	Subject Matter Expert
SOP	Standard Operating Procedure
T&E	Test & Evaluation

Appendix C: REFERENCES

"Simulation-based Evaluation of the Impact of Cyber Actions on the Operational C2 Domain", Paulo C.G. Costa, Ph.D., Associate Professor, Department of Systems Engineering and Operations Research / C4I Center/ Center for Air Transportation Systems Research

"Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service"; OMB Approval of Information Collection, https://federalregister.gov/a/2010-19809

BRAZIL. ICA 100-12: Regras do Are Servicos de Trafego Aereo. Rio de Janeiro, Brazil, April 2009.

Cisco 2014 Annual Security Report

"Exploring Potential ADS-B Vulnerabilities in the FAA's Nextgen Air Transportation System Graduate Research Project", Air Force Institute of Technology, Donald L. McCallie, BS, MS Major, USAF, http://www.hsdl.org/?abstract&did=697737

http://www.radartutorial.euhttp://www.oig.dot.gov/sites/dot/files/ADS-B_Oct%202010.pdf
"Hackers + Airplanes No Good Can Come Of This", Defcon 20, Brad "RenderMan" Haines, CISSP

Unity Game Development: Welcome to the 3D world
http://www.packtpub.com/article/unity-game-development-welcome-to-3d-world Will Goldstone, September 2009

U.S. National Security Alliance, http://staysafeonline.org/

U.S. Multi-State Sharing and Analysis Center, http://msisac.cisecurity.org/

VR-Link for Unity Users Guide 2013 Revision VRU-1.1-1-130801

VR-Forces Users Guide 2013 Revision VRF-4.2-1-131022

VR-Forces Scenario Management Guide 2013 Revision VRF-4.2-18-131022