Design of a Transoceanic Cable Protection System

Isaac Geisler, Kumar Karra, Felipe Cardenas, and Dane Underwood

***Abstract*—A system of underwater fiber optic cables spans the world's oceans, carrying 99% of all international communication data. This includes Internet traffic, phone calls and even text messages. There are 343 cables that span over 500,000 miles on the seafloor. Telecommunication companies invest billions of dollars into this network, causing it to grow by 36% each of the last 7 years.**

These cables are damaged and cannot deliver bandwidth over 150 times per year. Up to 20% of the causes of cable damages are unknown. Another area of concern for not just cable owners, but governments as well, is the threat of intentional sabotage and espionage.

This paper describes a design to protect these cables as well as the design of a Command Center for cable protection. The Command Center includes three functions: (1) Threat Identification Service, (2) Damage Prevention Service, and (3) Cable Repair Coordination Service. The Threat Identification Service will employ various technologies, such as satellite tracking and underwater sensors to detect nearby threats. The data obtained from these will be relayed to the Command Center. Next, the Damage Prevention Service will use the incoming data and send messages to appropriate authorities to attempt to prevent the damage from occurring. If damage does occur, the Cable Repair Service will record fault data and send this information to cable repair companies, expediting the repair process, thus reducing total cable downtime.

A model was built for this system, simulating threats entering a cable area and the probability of the technology alternatives detecting the threats. Recommendations will be made based on the simulation to provide the best technology alternatives needed to protect the cables.

I. Introduction

A system of underwater fiber optic cables spans the world's oceans. These submarine cables transmit 99% of all international communication data – this includes internet traffic, phone calls and even text messages. There are 344 cables [1] in service right now, with dozens more planned or coming online in the next few years. Cables are the most cost-effective alternative for long-distance telecommunications, offering high bandwidth at a fraction of the cost of satellite or microwave systems. There are over 500,000 miles of cables on the seafloor, and individual cables can be over 3000 miles long. Cables can cost anywhere from tens of millions to billions of dollars to construct and maintain [8][9]. They come in a variety of capabilities, and the current network consists of a patchwork of technologies, with many cables from the early 1990s still in service [10].

Given their importance and cost, the cables are surprisingly under protected. There is virtually no monitoring of the system, and most actions taken are purely in reaction to cable damage incidents. This damage is also more often than expected, with a cable fault occurring approximately every 3 days [11]. Cables are largely damaged accidentally by human activity, but they are also vulnerable to natural events, component failures and hostile human action. Cable faults are difficult and costly to repair, with repairs often taking weeks and costing millions of dollars [11][12].

II. Cable System Overview

A. Context Analysis

This cable network exists to deliver bandwidth across the world. Billions are invested every year by the global telecommunications industry to build new cables and maintain the current network. The current network of 344 cables can be divided into 7 major subsystems. These are the Transatlantic, Transpacific, Pan-east Asian, South Asia and Middle East Intercontinental, North and South American, Australia and New Zealand Intercontinental, and the Sub-Saharan African Intercontinental. The capabilities, growth, costs and threats vary significantly from region to region [13].

The total worldwide bandwidth of the network is approximately 87 Tbps [13]. Individual cables are capable of 10 to 400 Gbps of bandwidth, depending on age and technology [13]. New technologies have been tested with capacities of over 1 Tbps. Using these new cables, new systems are being developed and implemented to increase the global bandwidth from 87 to 742 Tbps over the next 10 years [13]. Bandwidth on these networks is rented out by the cable industry to land-based ISPs, other telecommunication industries, governments, technology companies and the finance industry. The standard retal unit used for pricing is 10 Gbps per month [14]. Prices vary from $25,000 to $250,000 per 10 Gbps per month, depending on the region and available bandwidth [6][14][15].

Cables are protected with various layers of armoring and insulation. The protection of these cables vary according to depth. In waters of less than 2000m depth, up to 3 alternating layers of steel armoring and additional insulation are added to the cables [10]. This is to protect the cables from potential damage from various threats. The armor adds

Manuscript received December 9, 2015. This work was supported in part by Raytheon Corporation. All authors are students at the Volgenau School of Engineering, Department of Systems Engineering and Operations Research, George Mason University, Fairfax, VA 22030 USA.

I.Geisler(email:ggeisler@gmu.edu),F.Cardenas(email:fcarden2@gmu.edu),K.Karra(email:skarra@gmu.edu),D.Underwood(email:dunderw@gmu.edu).

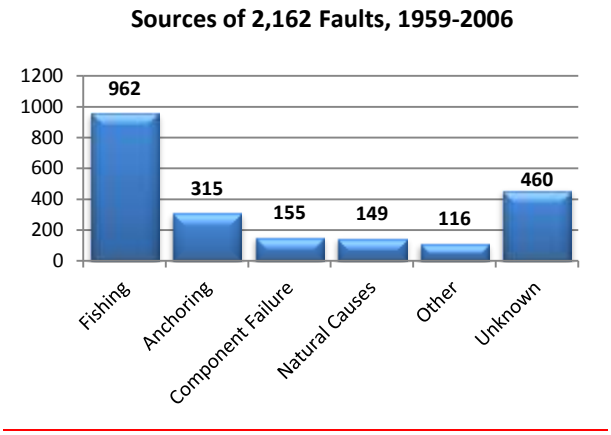

Fig. 1 Partial cable fault causes from 1959 to 2006

significant cost and weight to the cable and the installation process.

Cables are exposed to many threats and damage is frequent, as shown in Figure 1. Damage is divided into two large categories, external aggression faults and internal faults. External aggression is further decomposed into human and natural causes. By far the most common cause of cable damage is external human aggression, accounting for up to 80% of cable faults [10]. The vast majorities of these incidents are accidental and caused by fishing and anchoring. Intentional or hostile human action is also a real threat, although it is currently very difficult to determine with the current lack of system monitoring.

A major obstacle to reducing cable faults or preventing other problems is the lack of information. There is no global monitoring or reporting system in place, so analysis of cable faults is difficult. The FCC has recently acknowledged the size of the problem and has recently mandated new rules requiring all US submarine cable operators to log and report all cable faults [7].

Once a cable is damaged and the location is determined, repairs can begin. The first step is to contact a repair company and hire a cable repair ship. Some submarine cable operators are vertically integrated with their own cable repair ships, but many are not and rely on hiring outside contractors. Depending on the cable operator, region of the affected network and location of the fault, it can take weeks for a repair ship to be contracted and travel to the fault site [10][12].

Repair operations under perfect conditions and no complications take 3-5 days and cost $3+ million [12]. Repairs can be significantly delayed by many factors such as weather, difficulty finding the cable, or errors in reinstallation. In all, typical downtime for cable faults is measured in weeks. During this time, cable owners face significant losses due to repair costs, and the loss of cable bandwidth, which can be very expensive.

B. *Stakeholder Analysis*

Primary stakeholders are identified as those entities which have a direct interaction with the submarine cable system or TCPS. Secondary stakeholders are identified as those entities which would face significant disruption as a result of the modification of either the submarine cable system or TCPS.

1) Primary Stakeholders

Alcatel-Lucent (47% market share) is the largest company in the submarine cable installation/maintenance industry [1]. However, the majority of their business comes from the production of fiber-optic cables along with many other businesses such as aviation, financial services, healthcare, energy production, etc. [2] Their objectives, with regards to the cable system, would include the expansion of the cable system along with benefitting from a high fault rate of the cables, although, the first objective would have priority because of its relative contribution to its business. [2]

TE, SubCom (30% market share) is the second largest company in the industry. [1] They are a direct competitor to Alcatel-Lucent, as a result, engage in many of the same areas of submarine cable maintenance/installation. Similar to Alcatel-Lucent, TE has the majority of its business centered around cable production and various other industries. [3]

NEC, Submarine Systems (12% market share) is the final major competitor in the industry [1]. The objectives of NEC are identical to the previous two companies with regards to the submarine cable industry as they focus heavily on cable manufacturing and installation over repair. Furthermore, the submarine division is a small percentage of its overall business [4].

As of 2013, 80% of cable ownership resided with consortiums of telecommunication companies [1]. The objective of these consortiums are to have uninterrupted data transmission through these lines at minimal costs. Furthermore, as a result of the over-expansion of the early 2000s, telecom companies are focusing on enhancing existing cables over building new ones [1].

2) Secondary Stakeholders

Insurance company interests are directly in line with the telecommunication companies and the other owners, in that, they all have a financial stake in the optimal running of the cable system.

Large Technology companies and financial institutions heavily rely on the cable system for daily operations of their businesses. Therefore, a high value would be placed on the optimal functioning of the system.

C. *Problem Statement*

Undersea cables carry almost all of international data communications and it costs millions to lay new ones. Despite the massive dependence on these cables, they are left unguarded. This threat can lead to negative effects on the security, economy, politics of companies, institutions, and governments affected. More than a 150 cable faults occur every year and about 86% are caused by external human aggression. Around 21% are caused by accidental causes such as anchor drops and fishing incidents. However, there are increasing fears of sabotage and espionage by malicious groups due to reported incidents. In addition, the ability to

detect and repair faults is slow and costly, with an average 20.6 days of down time for repair and about $6 million lost for each cable.

D. Need Statement

There is a need to increase surveillance of cables in order to decrease the number of faults, increase the rate of detection, and improve the mean notification time of damaged cables.

Making the investment in an underwater surveillance allows cable-operating companies to potentially identify threats preemptively and prevent them from happening. This inadvertently minimizes cable damage, decreases the cost in repairing cables, and deters future threats from happening. In addition, cable down time is minimized by increasing fault reaction time, which lessens the cost of lost bandwidth. Cable operators can also protect the value of investment through long-term savings in cost, which allows for allocating resources in installing new underwater cables or improving cable technology.

E. Performance Gap

The current process of underwater surveillance is underdeveloped and fails to protect the underwater cables. Over 100 cable fault incidents are occurring every year, with each fault incurring millions of dollars in lost bandwidth and repair costs [20]. Additionally, the repair process is slow and takes time to fully repair a cable. There are three steps to the repair process: notification of the cable damage, traveling to the fault location, and repairing the cable itself. The mean notification time of the cable damage is about 6 days [10]. The time to find a fault location can be anywhere from one day up to three weeks [10]. All of these delays are costing stakeholders' money.

Developing a process to ensure protection of these cables is the purpose of the Transoceanic Cable Protection System. Total protection of the cables may be infeasible due to the vastness of the oceans and the depths they reach. However, with a proper system alternative, we are aiming for a 30% reduction in cable damages each year. This will be done through better surveillance and most importantly, better communication to deter threats.

For the issue of current cable surveillance, the goal of our system is to be able to monitor 80% of the entire cable length. Ideally, we would want to monitor the entire cable. Due to extreme depths and unreachable places where these cables may be located, we have reduced this number. Monitoring the cable will also help identify threats and find damage locations faster, thus closing other performance gaps. Methods for how this surveillance will be done will be discussed in the design alternatives section.

III. Operational Concept

The TCPS will have three primary goals when it is put into place: identification, prevention, and organization of repair. The overarching goal of the system is to first prevent damage from happening. If damage does occur, reducing cable downtime is the next objective of the system. Because there are two separate problems we are facing (accidental and intentional threats), there must be mitigation strategies for both systems.

The diagram below shows the current process of the cable system. First, a threat enters a cable area. Either the threat causes the fault or it does not cause the fault. If the threat does not cause a fault, the cable continues its service. If the threat does cause a fault, three things must happen following the event of a damaged cable. In the first block, the cable owner must find the fault location and contact a repair ship. Next, the repair ship must travel to the fault location. This step takes time because the repair ships do not know exactly where the cable fault occurred, so they will spend time searching for the damaged section. Lastly, the repair ship repairs the cable and the cable is back in service.

Fig. 2 Current repair process

The next figure table shows where our system will be implemented in the current system. Each function will operate in its respective area. The identification and prevention functions will occur after the threat enters the cable area. The repair organization function will happen if the system is not able to prevent damage.

Fig. 3 The Transoceanic Cable Protection System (TCPS) implemented in the current system

Identification is the first step to preventing cable damage from occurring. Within this function, the system will identify three things: surface-level threats, underwater threats, and fault locations and extent of the cable damage. As mentioned in the problem statement, 21% of the threats that cause cable damages are unknown. Identifying surface-level threats, such as shipping vessels and fishing vessels, will be done through better communication. The method through which our system will accomplish this task will be discussed in the design alternatives.

Identifying underwater threats, such as saboteurs or espionage devices, will be much more difficult to detect because the ocean is so large and monitoring anything underwater is an extremely difficult task. Identifying fault location and the extent of the damage will be given directly to cable repair companies so that they can quickly travel to the site and quickly begin the repair process, thus reducing cable downtime.

Prevention of cable faults will stem from two aspects, forecasting and communication. Based on our research, we know that the majority of cable faults occur in depths less than 200 meters and are more common in certain regions [12]. For example in Southeast Asia, large amounts of fishing activity occur daily. By knowing that volume will be higher in this region, we can forecast that it is more likely for cable faults to happen. In this case, the system would heavily monitor all ship activity near cable protection zones. Simply monitoring ship activity, however, would not serve much of a purpose without communication.

Alerting these ships of their proximity to cable areas and instructing them to refrain from trawling or dropping anchor could potentially reduce cable faults. The operational concept is to prevent damage before it happens by monitoring this traffic. With regards to the intentional human action, the system may not be able to prevent the damage, but it very well could serve as a deterrent. If a threat is aware that there is surveillance, they would be less likely to attempt sabotage for fear of getting caught. If possible, detecting underwater threats and quickly notifying authorities could potentially prevent a fault from happening. This entire prevention operation stems from the identification operation.

The entire project encompasses the need to perform these functions from a central location. Our operational concept to do this will be a physical Mission Control Center. All information obtained from the TCPS alternatives will be sent to mission control. Examples of this include marine traffic data and subsea monitoring data. Using this data, the system will identify threats to the cables. With this threat data, prevention of damage will occur through either messages to marine traffic or messages to appropriate authorities. These messages will be sent from Mission Control for faster communication. If damage is not prevented, Mission Control will begin the third function, organization of the repair process, which will involve sending messages to repair companies. This mission control will be the basis for the entire project as the TCPS system, either underwater or surface level, will be operated from this location. This operational concept is shown in Figure 4.

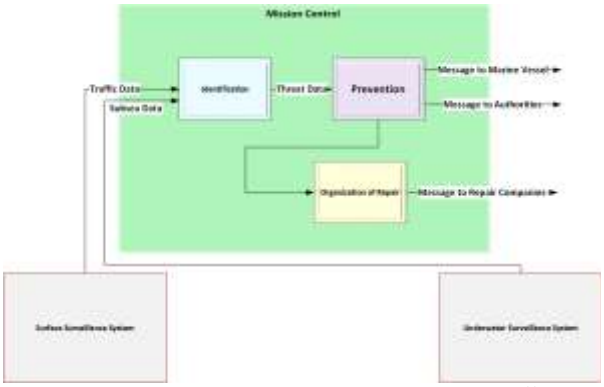

Fig. 4 The mission control center will receive and analyze traffic and data and subsea monitoring data to identify threats. Identified threats will be attempted to be prevented. If damage is not prevented, the repair effort is organized.

IV. Design Alternatives

There are design alternatives for each of the three major functions from the Operational Concept. For the identification functions, design alternatives are divided into two categories: Surface Identification and Underwater Identification. Within these two alternatives are technologies that will be used to meet requirements. These technologies will be discussed in their respective sections. Prevention and repair organization functions each have alternatives, mostly relying on communication from Mission Control.

A. Surface Identification Alternative – Marine Traffic Monitoring and Warning (MTMW)

Tracking commercial ships that are in the area of a cable fault also provides an immediate list of ships to further investigate to determine cause and liability. In many cases of fishing or anchoring caused faults, the culprit ships are never identified. When identified, these ships could then be pursued for repair costs and fines. If ships are more regularly held accountable for damaging cables, it may cause other ships to be more cautious, thereby deterring activities in areas with cables that are causing cable faults.

1) Automatic Identification System

Automatic Identification System (AIS) transponders are required equipment on all vessels over 299 tons. These devices relay a ships position, speed and identification every 2 seconds to 3 minutes to AIS shore receivers [16]. Class A receivers can also receive text messages and warnings. AIS devices have ranges of 50-100 nautical miles to terrestrial receivers, but there is also a growing satellite network with AIS receivers that will greatly increase their range [17].

2) Marine Very High Frequency Radio

All ships over 20 meters in length are required to have Marine Very High Frequency (VHF) radios aboard. They are also required to monitor channel 16 at all times for safety and emergency information. VHF range varies with conditions, but is typically 100-200 nautical miles [17].

B. Underwater Identification Alternative

Because the Surface Identification Alternative only monitors surface-level activity, there is a need for an alternative to fill the gap of underwater identification. This will be done through various sonar sensors as well as "Platform Alternatives", which will be a vehicle or device on which the sonar will be integrated. A platform will be an Autonomous Underwater Vehicle (AUV), Remote Operated Vehicle (ROV), or a Sonar Network (SonarNet). These platforms are useless without a sonar system, which will allow the platforms to record data and maneuver through the water.

1) Active Sonar Alternatives

Active sonar operates by transmitting sound energy from a transducer and listens for the return "echo" that comes from the sound energy bouncing off of objects. Active sonar is widely used for scanning seabed to create topographical

maps or searching for shipwrecks. It is generally used when the system is anticipating a target or "actively" searching for an object. The three active sonar alternatives are Synthetic Aperture Sonar, Compressed High Intensity Radar Pulse, and Side-scan and Multibeam Sonar.

a) Synthetic Aperture Sonar (SAS)

SAS provides very high-resolution (up to 10 times higher than Side Scan and Multibeam sonar) images and can provide data in real time to monitors. One of the most attractive capabilities of SAS is that it can produce images of the seafloor along with bathymetry information.

b) Compressed High Intensity Radar Pulse (CHIRP)

CHIRP sonar is widely used in the fishing industry to locate schools of fish. Unlike SAS and other sonars that emit a constant signal, CHIRP sonar emits bursts of sound energy. Doing this helps to make up for the inconsistent echo, or backscatter, that fish create.

c) Side-scan and Multibeam Sonar (SSM)

Side-scan and Multibeam sonar is a relatively old technology, but is one of the most trusted and reliable sonars on the market. Similar to SAS, the side-scan portion of the system emits sound energy in a wide fan shape, and the return echo provides detailed imagery of a seafloor or object. Side-scan, however, cannot provide bathymetry information and must be used along with multibeam sonar. Multibeam emits a narrow signal and the return echo is converted into depth information.

2) Passive Sonar Alternatives

Unlike active sonar that emits a signal and listens for the echo, passive sonar emits no signal and listens for the signals from other objects. It can detect engine and propeller noise from submarines, marine life, and even the air bubbles that burst from a diver or engine. Passive sonar systems can be extremely sensitive and used in almost any location. They are robust and are currently being used all over the world on submarines.

a) Hydrophones

Hydrophones are essentially listening devices that sense objects creating noise. They are widely used on submarines for defense purposes. For example, a submarine may use a hydrophone to listen for nearby submarines.

3) Platform Alternatives

To put the active or passive sonar technologies into use, they must be carried by a platform. For this project, we are considering three alternatives: Autonomous Undersea Vehicles, Remote Operated Vehicles (ship-towed), and Sonar Networks. Decision criteria will be based on cost, effectiveness, and capabilities.

a) Remote Operated Vehicles (ROV)

ROVs are frequently used for oil pipeline inspection, bridge inspection, and survey missions. They are generally towed behind a ship and are attached to the ship by an Ethernet tether. These tether lengths can range from 150 meters to 10 kilometers. ROVs can be equipped with multiple technologies, such as sonar, cameras, lights or small tools. Benefits of ROVs are that one can travel to virtually any location, as the tether is the only restriction. They provide real time information due to the Ethernet tether and are a versatile piece of equipment. Drawbacks include the very high cost of towing an ROV by a ship.

Three ROVs will potentially be used as platforms: ASI Mohican, Oceaneering NEXXUS, and Oceaneering Millennium Plus.

i) ASI Mohican

The ASI Mohican is a ship-towed ROV. It is a large-scale inspection system. It has a water depth rating of 2000 meters and a 10 km tether, allowing a large range of inspection [23].

ii) Oceaneering NEXXUS

NEXXUS by Oceaneering is a ship-towed ROV, specializing in intervention capabilities. It has a water depth rating of 4000 meters and has a 450 kg (1000 lb) payload [24].

iii) Oceaneering Millennium Plus

Similar to the NEXXUS, the Millennium Plus also has a 4000 meter depth rating. It is also equipped with a powerful propulsion system. This is one of Oceaneering's best ROVs on the market. The Millennium Plus also contains High-Definition cameras, which could be useful for the TCPS system.

b) Autonomous Undersea Vehicles (AUV)

Autonomous Undersea Vehicles are applied in many different situations, whether it is mapping seafloors at depths humans cannot safely reach, or patrolling a port checking for mines or hazardous materials on ships. AUVs come in different shapes and sizes, but are categorized in four groups: Man-operated, Light Weight Vehicle, Heavy Weight Vehicle, and Large Vehicle classes. They are capable of being equipped with sonar technologies, either passive or active sensors.

Five AUVs were researched for the project: Kongsberg Seaglider, Raytheon AN/AQS-20A, Kongsberg REMUS 6000, Kongsberg HUGIN, and Lockheed-Martin Marlin Mk3. The table below shows specifications necessary for our system and simulation (speed, duration, and depth rating). These AUVs have other capabilities, but these physical

AUV	Speed	Duration	Depth Rating
Kongsberg Seaglider	0.25 m/s	7200 hours	1000 meters
Kongsberg REMUS 6000	2.3 m/s	22 hours	6000 meters
Kongsberg HUGIN	3.1 m/s, 2.1 m/s	74, 100 hours	6000 meters
Raytheon AN/AQS-20A	Unknown	Unknown	Unknown
Lockheed-Martin Marlin Mk3	3.1 m/s	60 hours	4000 meters

Fig. 5 AUV alternatives summary

specifications are most important to us for the scope of our project.

c) Sonar Network (SonarNet)

Sonar Networks are groups of acoustic sonar sensors arranged in such a way that they provide coverage of a specified area. In the case of Sonar Networks, sensors would be strategically placed along or near the cables to allow for localization and triangulation of threats or objects. This network would provide excellent coverage due to the exceptional range of hydrophones and other sonar sensors. The effectiveness of this system will depend on the exact range of the sonar, number of nodes, and communication with on-shore or ship-based monitors.

C. Prevention Alternative

To perform the second function, prevention, there must be a system from which we can communicate with outside entities in order to prevent a threat from causing damage. Mission Control will have a big role in this function. All identification alternatives (Surface and Underwater) will relay data on threats to Mission Control. The surface identification alternative will relay this data through marine traffic monitoring using AIS transponders. Underwater identification alternatives will send the messages via satellite from the AUV, ROV, or SonarNet. After Mission Control has received this data, it will send messages to appropriate entities based on threat type. Messages will be sent to marine traffic through VHF radio in order to prevent accidental damage. Mission Control will alert them of their proximity to cables and warn them not to drop anchor or to raise their fishing nets. Whether they follow orders or not, we cannot control. However, due to the system identifying the threat, we will know which ship caused the damage.

D. Repair Organization Alternative

In the case that a fault has occurred, TCPS will relay fault type and location data to Mission Control. Mission Control will then send this information to cable repair companies. By knowing this information, repair companies will spend less time searching for broken cables and will know the extent of the damage. This alternative aims to significantly reduce location finding time and repair notification delays.

V. Simulation

A. Simulation Overview

The goal of our simulation is to determine which alternative or combination of alternatives provides the best utility for a given cable surveillance case. Utility will be determined by a combination of factors: cost, probability of detecting faults, probability of detecting espionage or tampering, and probability of identification of threats and fault causes.

Cables are operated in a large variety of environments, and each cable is somewhat unique. This leads to large difficulties in creating a simulation that can accurately model a particular cable. Instead, we have decided to select a few representative cables to model specifically to give more accurate data for that cables and others like it. This also gives us the benefit of specifically modeling the exact bandwidth capacity and rental rates of that particular cable. We will also contact the cable owner for more information on their cable.

Once a cable is modeled, our next step is to simulate threats and faults on that cable system. Since threats are not currently tracked or monitored, we had to develop a way of modeling potential threats from known fault data. This required several assumptions on the conversion rate of specific threats to actual faults. Next, we determined inter-arrival times of these threats for a single cable system.

The threats modeled by the simulation are fishing, anchoring, component failure, natural causes, espionage and sabotage. The proportion of these threats is based on their fault proportion and our expected threat-fault conversion rate. If a fault occurs, cable downtime, repair time, lost bandwidth cost and repair cost are generated from distributions based on research data.

Our design alternatives are also modeled by the simulation. Parameters for movement speed, movement range, sonar scanning/listening range, number of units are determined for each alternative and programmed into the simulation. Alternatives are split into 3 broad categories: active alternatives (e.g. AUV/ROV), passive alternatives (e.g. hydrophones/sonar network), and surface alternatives (e.g AIS/VHF communications).

The simulation is then run for 10 years, with all threats and TCPS design alternative agents being updated on an hourly clock. Threats and TCPS agents are generated and placed on the modeled cable. As the hourly clock ticks, TCPS agents are moved (if capable) along the cable in patrol paths, and threats are converted into faults based on our postulated threat-fault conversion rate. All data generated by the simulation on threats, faults, downtime, costs and TCPS agents is output to a text file.

Each simulation is then replicated 7700 and the aggregate data is used for analysis. The number of 7700 replications was found by calculating the number of replications we would need for a 95% confidence interval based on the mean and standard deviation of all parameters from a 1000 replication initial run.

B. Design of Experiment

Inputs	Cable	Active Alt(s)	Passive Alt(s)	Surface	Replications
1	FLAG Atlantic-1	None	None	None	7700
2	FLAG Atlantic-1	Seaglider AUV w/ SAS	None	None	7700
3	FLAG Atlantic-1	Remus 6000 AUV w/ SAS	None	None	7700
4	FLAG Atlantic-1	None	Hydrophone	None	7700
5	FLAG Atlantic-1	None	None	AIS System	7700
6	FLAG Atlantic-1	Seaglider AUV w/ SAS	Hydrophone	None	7700
7	FLAG Atlantic-1	Seaglider AUV w/ SAS	None	AIS System	7700
8	FLAG Atlantic-1	Seaglider AUV w/ SAS	Hydrophone	AIS System	7700
9	FLAG Atlantic-1	Remus 6000 AUV w/ SAS	Hydrophone	None	7700
10	...	...	...	...	...
11	Tata TGN	None	None	None	7700
12	Tata TGN	Seaglider AUV w/ SAS	None	None	7700
13	...	...	...	...	...

Fig. 6 – Design of Experiment showing combinations of alternatives.

C. Simulation Diagram

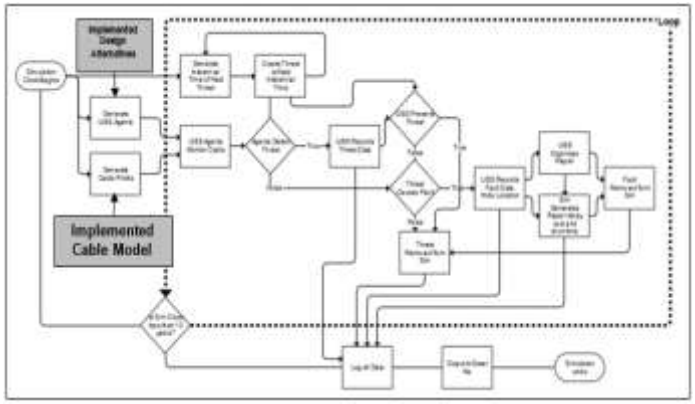

Fig. 7 – Diagram of main simulation loop and flow of data.

D. Simulation Parameters

For our first cable, we modeled the FLAG Atlantic-1 (FA-1) cable system. Using bathymetric maps from NOAA, we estimated the depth through the range of the cable and used a few equations to model the cable in Java as an array. The cable is modeled on a per km basis, and each block of the array represents the approximate depth of the cable in meters at that km. The FA-1 cable runs for a total of 14,500 km, has 4 cable-landing stations, and a maximum depth of 6000m.

For threat inter arrival times, first we calculated the rate of faults for a single cable. Unfortunately, we only have aggregate data for the entire worldwide cable system for fault numbers. Fault/threat rates and occurrences for individual cables are either not logged at all, or not made public, except for extraordinary or unusual cases. Cable owners don't like to publicize interruptions in their services.

Based on the global data of 343 cable systems, and 150+ faults per year, we've estimated the fault rate for a single cable to be approximately 0.5 faults per cable per year, or 5 faults over a 10-year period. Next, we estimated the threat to fault conversion probability for our 6 fault types. Due to the lack to threat monitoring, we made estimations based on the danger each threat presents to the cable system. For example, purposeful sabotage will result in a fault 100% of the time, while accidental faults from fishing equipment will have a much lower rate (we've estimated 5%). Using these numbers, we can calculate the threat interarrival time in hours for threats on a single cable.

	Probability of Fault Type	Normalized Probability of Fault type	P * 0.5 faults/year	Threat-Fault conversion probability	Threats per year of each type	Threat Interarrival rate in hours
Fishing	0.444	0.541	0.2704	0.05	5.408	1619.8
Anchoring	0.156	0.190	0.0950	0.25	0.380	23051.2
Component	0.072	0.088	0.0438	1.00	0.044	199776.7
Natural	0.069	0.084	0.0420	0.10	0.420	20846.3
Espionage	0.04	0.049	0.0244	0.00	0.024	365000.0
Sabotage	0.04	0.049	0.0244	1.00	0.024	359598.0
Total	**0.821**	**1**	**0.5**	**2.4**	**6.300**	**1390.4**

Table used to determine threat interarrival rate

E. Preliminary Simulation Results

So far, we have completed simulation on the as-is case for the FA-1 cable. This represents the expected number and type of faults, and associated costs for a transatlantic cable over a 10 year period.

	Threat Type					
	Fishing	Anchoring	Component	Natural	Espionage	Sabotage
Mean per 10 years	56.65	4	0.47	4.68	0.66	0.2

Number of threats per 10 years

	Totals				
	Threats	Faults	Downtime (hrs)	Repair Cost	Lost Bandwidth Cost
Mean per 10 years	66.65	4.11	1236.63	$9,971,023.31	$10,107,639.98
Mean per Fault			301	$2,426,960.00	$2,460,212.67

Total threats, faults, downtime and costs

F. Validation

The approach to the validation of our simulation model will consist of two parts: the validation of the "as-is" simulation model and the validation of the simulation model containing the design alternatives of the TCPS system. For the "as-is" simulation, the output results can be compared to the data that we have acquired through our research of current the fault statistics. This data will be compared using a two-tailed z-test to determine if there is any significant difference between the two data sets. For the simulation model containing the design alternatives of the TCPS system, there is no corresponding statistical test that we can perform for the validation. This is because the system is currently theoretical and, therefore, there is no data available on the real-world performance of such a system. Given this constraint, there are a few methods we can employ for reducing the risk of the simulation being incorrect. These include, ensuring that the "as-is" simulation is accurate and is consistent with the real world situation it is modeling. Furthermore, we must clearly layout all the assumptions of the TCPS simulation along with the parameters of the simulation so that anyone using the simulation is clearly aware of how the simulation functions and any potential limitations it might have.

G. Utility

Given our choice to limit the simulation model to a few representative cables that can adequately capture the nature of most of the cables around the globe, our approach to utility can be broken down into specific stakeholder-based analysis. Through our research, we have concluded that there are four main areas that must be considered when determining the utility of a design alternative. These are: prevention, identification, downtime, and lifespan.

Prevention is the numerical ratio of the number of threats detected to the number of faults that occurred. For this criterion, the higher the number, the better. Identification is the number of treats detected over the number of threats that historically occurred in a given area. Downtime is the average amount of time that a design alternative is not operational or the maintenance time over the given lifespan of the system. In our case we are designing the system to have a lifespan of approximately 10 years. Finally, the lifespan is the amount of time the design alternative able to operate without significant modification or replacement. Tentatively, we have set this to mean either a total replacement of the system or a modification that costs greater than 50% of its original acquisition cost. Each of these criteria can be further broken down into more specific categories as we learn more about the specific stakeholder needs of a given gable. These four criteria will be compared to cost in order to find the highest utility design alternative.

VI. Future Work

Over the next several weeks, we will be working on implementing the design alternatives into the simulation. This will help us understand the best options for different cables. This will lead us into an in-depth trade-off analysis for TCPS based on our utility function.

Additionally, we are working on getting cost information from manufacturers. This information is kept confidential due to competition between manufacturers. We plan on getting some cost and other information from our sponsor.

Lastly, we will continue to improve our business model, which is an integral part of the Mission Control Center. We plan on running a Monte Carlo analysis for the cost functions in order to obtain an accurate ROI.

References

[1] TeleGeography. (2015, September 15). Submarine Cable Map [Online]. Available: http://www.submarinecablemap.com/#/

[2] Reuters. (2015, August 26). Libya's land phone line system breaks down after cables were damaged [Online]. Available: https://www.dailystar.com.lb/News/Middle-East/2015/Aug26/312843-libyas-land-phone-line-system-breaks-down-after-cables-were-damaged.ashx

[3] J. Kirk. (2013, March 27). Sabotage suspected in Egypt submarine cable cut [Online]. Available: http://www.computerworld.com/article/2495954/internet/sabotage-suspected-in-egypt-submarine-cable-cut.html

[4] F. Cahyafitri and R. Cahyafitri. (2013, June 29). Indosat spends Rp 10 billion replacing stolen underwater cable [Online]. Available: http://www.thejakartapost.com/news/2013/06/29/indosat-spends-rp-10-billion-replacing-stolen-underwater-cable.html

[5] Malta Today. (2011, November 14). Damaged GO submarine cable repaired [Online]. Available: http://www.maltatoday.com.mt/news/national/13804/damaged-go-submarine-cable-repaired#.Vhkz3_lViko

[6] M. Islam. (2015, May 8). Submarine Cable plans to sell bandwidth to Italian firm at low price [Online]. Available: http://www.thedailystar.net/business/submarine-cable-plans-sell-bandwidth-italian-firm-low-price-80342

[7] J. Hawn. (2015, September 18). FCC considers new rules for submarine cables [Online]. Available: http://www.rcrwireless.com/20150918/policy/submarine-cables-may-get-new-fcc-rules-tag15

[8] L. Hedges. (2015, March 19). Top five telecoms projects [Online]. Available: http://www.hibernianetworks.com/corp/wp-content/uploads/2013/02/Top-five-telecoms-projects-2015_Capacity-Magazine_April-2015.pdf

[9] F. Lardinois. (2015, May 11). Microsoft invests in 3 undersea cable projects to improve its data center connectivity [Online]. Available: http://techcrunch.com/2015/05/11/microsoft-invests-in-3-undersea-cable-projects-to-improve-its-data-center-connectivity/#.hhwwya:w2DQ

[10] L. Carter et al. "Submarine cables and the oceans: connecting the world" UNEP-WCMC/UNEP/ICPC. Cambridge, UK, Biodiversity Series No. 31, 2009.

[11] L. Carter and D. Burnett. (2011). About Submarine Telecommunications Cables [Online]. Available: https://www.iscpc.org/documents/?id=1752

[12] W. Rain. (2009, December 14). Problems faced by Industry in the repair of damaged submarine telecommunications cables inside maritime jurisdictional claims [Online]. Available: http://cil.nus.edu.sg/wp/wp-content/uploads/2009/10/Wolfgang-Rain-Session-3.pdf

[13] Y. Ruggeri et al. "Submarine Telecoms Industry Report" Terabit Consulting. Cambridge,MA, Issue 3, 2014.

[14] "Global Bandwidth Research Service Executive Summary" TeleGeography. Washington D.C. 2015

[15] "Australia & Pacific Bandwidth Review" TeleGeography. Washington D.C. February, 2015.

[16] US Coast Guard. (2010, July 13). Types of Automatic Identification Systems [Online]. Available: http://www.navcen.uscg.gov/?pageName=typesAIS

[17] "Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band" Intl. Telecommunication Unit – Radiocommunication, Geneva, Switzerland, Recommendation, ITU-R M.1371-4, April 2010.

[18] Kokusai Cable Ship Co. (2010) Optical Submarine Cable Repair Method [Online]. Available: http://www.k-kcs.co.jp/english/solutionRepairingMethod.html

[19] D. Burnett. Submarine Cables: The Handbook of Law and Policy. Boston, MA: Martinus Nijhoff, 2014.

[20] A. Chang. (2013, April 2). Why Undersea Internet Cables Are More Vulnerable Than You Think [Online]. Available: http://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/

[21] O. Khazan. (2013, July 16). The Creepy, Long-Standing Practice of Undersea Cable Tapping [Online]. Available: http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

[22] W. Landay, "The Navy Unmanned Undersea Vehicle (UUV) Master Plan," Nov. 2004. [Online]. Available: http://www.navy.mil/navydata/technology/uuvmp.pdf

[23] "Side Scan Sonar." NOAA's Office of Coast Survey. 2015. [Online]. Available: http://www.nauticalcharts.noaa.gov/hsd/SSS.html.

[24] "Harbor Monitoring Network System." NEC.com. N.p., 2015. Web. 31 Aug. 2015. http://www.nec.com/en/global/solutions/safety/critical_infra/harbormonitoring.html.

[25] "Harbor Monitoring Network System," NEC, 2015. [Online]. Available: http://www.nec.com/en/global/solutions/safety/critical_infra/harbormonitoring.html.

[26] "Autonomous Underwater Surveilance System Network," L3 Oceania, 2014. [Online]. Available: http://www2.l-3com.com/oceania//products/maritime_aussnet.htm.

[27] "ROV Fleet," ASI-Marine, 2015. [Online]. Available: http://www.asigroup.com/system/assets/attachments/000/000/181/original/ROV_Fleet.pdf.

[28] D. Main. (2015, April 2). Undersea Cables Transport 99 Percent of International Data [Online]. Available: http://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072

[29] S. Whitehead. "Submarine Cable Testing" Anritsu Corp., Richardson, TX, Application Note MW90010A, Dec. 2010.

[30] D. R. Burnett, "Recovery of Cable Repair Ship Cost Damages from Third Parties That Injure Submarine Cables," *Tul. Mar. L.J.*, vol. 35, p. 103, 2011 2010.

[31] A. Palmer-Felgate *et al*. "Marine Maintenance in the Zones - A Global Comparison of Repair Commencement Times" presented at the SubOptic Conference Presentation, Paris, France, May 2013.
[32] G. White. (2014, November 20). *Spy cable revealed: how telecoms firm worked with GCHQ* [Online]. Available: http://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq
[33] B. Gertz. (2015, September 22). *Russian Spy Ship Makes Port Call in Caribbean* [Online]. Available: http://freebeacon.com/national-security/russian-spy-ship-makes-port-call-in-caribbean/
[34] D. Sanger and E. Schmitt. (2015, October 25). *Russian Ships Near Data Cables Are Too Close For U.S. Comfort* [Online]. Available: http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0
[35] L. Stewart. (2015, February 2). *20,000 leagues under the sea... a trawler hit an internet cable and sent broadband into meltdown* [Online]. Available: http://www.belfasttelegraph.co.uk/technology/20000-leagues-under-the-sea-a-trawler-hit-an-internet-cable-and-sent-broadband-into-meltdown-31009132.html
[36] M. Fachot. (April 2012). *Safety at sea from shore and space: Additional and improved international standards for maritime safety* [Online]. Available: http://iecetech.org/issue/2012-04/Safety-at-sea-from-shore-and-space
[37] ICPC. (May 2015). *Cableships of the World* [Online]. Available: https://www.iscpc.org/cableships-of-the-world/?items=0
[38] M. Ayers. Telecommunications System Reliability Engineering, Theory, and Practice. New York, New York: Wiley & Sons, 2012.