

# Design of a Transoceanic Cable Protection System

Technical Report

Isaac Geisler  
Kumar Karra  
Felipe Cardenas  
Dane Underwood

Faculty Advisor: Dr. Lance Sherry  
Sponsor: Mr. George Blaha, Raytheon

---

Department of Systems Engineering and Operations Research  
George Mason University  
4400 University Drive, Fairfax VA, 22030  
December 9, 2015

## Table of Contents

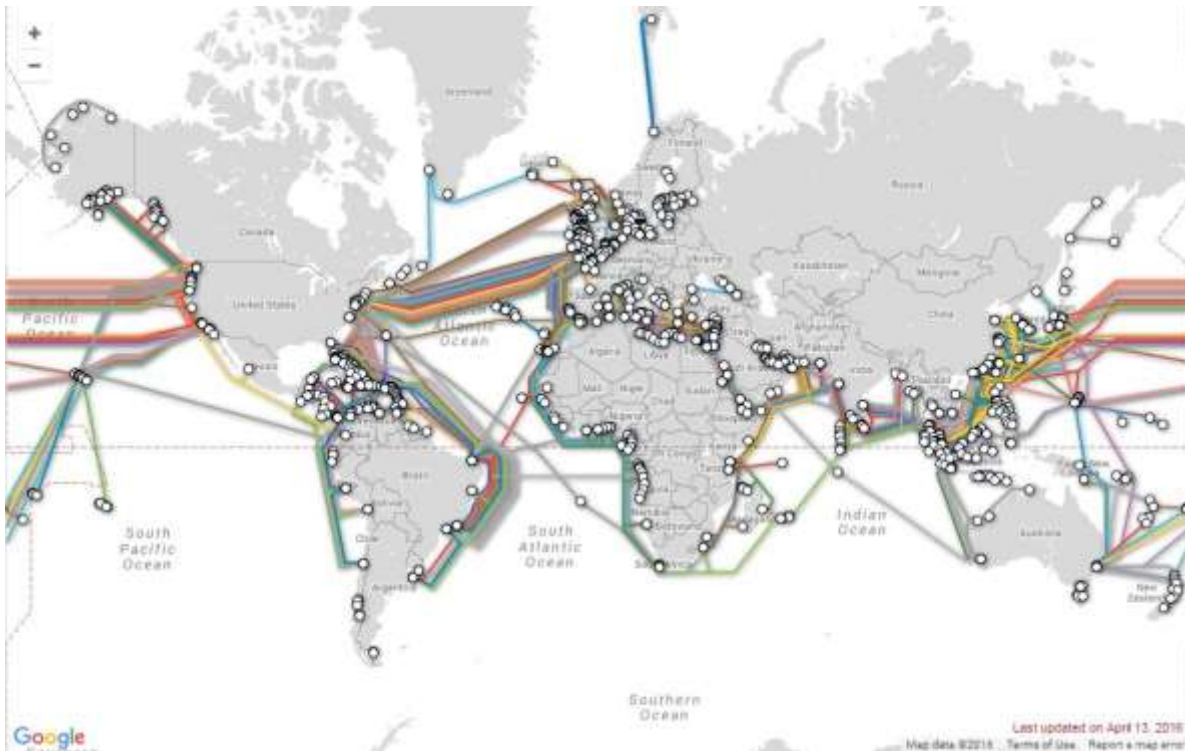
<b>1.0 Context Analysis.....</b>	<b>4</b>
1.1 Overview of Cable System.....	4
1.2 Cable Network as a Bandwidth Delivery Service.....	6
1.3 Cable Construction and Installation .....	8
1.4 Threats and Damage to Cables .....	10
1.5 Damage Detection and Location Finding.....	14
1.6 Cable Repair Process.....	15
1.7 Cable Protections .....	19
<b>2.0 Stakeholder Analysis .....</b>	<b>21</b>
2.1 Stakeholder Overview .....	21
2.2 Primary Stakeholders.....	22
2.3 Secondary Stakeholders .....	23
<b>3.0 Problem and Need.....</b>	<b>26</b>
3.1 Problem Statement.....	26
3.2 Statement of Need .....	26
3.3 Performance Gap .....	26
3.4 Operational Concept.....	28
<b>4.0 Requirements.....</b>	<b>32</b>
4.1 Mission Requirements .....	32
4.2 Functional Requirements .....	32
4.3 Design Requirements .....	33
<b>5.0 Design Alternatives .....</b>	<b>35</b>
<b>5.1 Surface Identification Alternative .....</b>	<b>35</b>
5.1.1 Automatic Identification System .....	36
5.1.2 Marine Very High Frequency Radio.....	36
<b>5.2 Underwater Identification Alternative.....</b>	<b>36</b>
5.2.1 Active Sonar Alternatives .....	36
5.2.1.1 Synthetic Aperture Sonar .....	37
5.2.1.2 Compressed High Intensity Radar Pulse.....	38
5.2.1.3 Side-scan and Multibeam Sonar .....	39
5.2.2 Passive Sonar Alternative .....	40
5.2.2.1 Hydrophones .....	40
5.2.3 Platform Alternatives .....	41
5.2.3.1 Remote Operated Vehicles .....	41
5.2.3.1.1 ASI Mohican.....	42
5.2.3.1.2 Oceaneering NEXXUS .....	42
5.2.3.1.3 Oceaneering Millennium Plus.....	42
5.2.3.2 Autonomous Undersea Vehicles.....	43
5.2.3.3 Sonar Networks.....	44
<b>5.3 Prevention Alternative.....</b>	<b>45</b>

5.4 Repair Organization Alternative .....	45
5.5 Alternatives Summary .....	46
<b>6.0 Simulation .....</b>	<b>47</b>
6.1 Simulation Overview .....	
6.2 Simulation Requirements .....	
6.3 Design of Experiment .....	
6.4 Simulation Diagram .....	
6.5 Simulation Parameters .....	
6.6 Simulation Results .....	
6.7 Sensitivity Analysis .....	
6.8 Validation .....	
<b>7.0 Business Case .....</b>	<b>81</b>
7.1 Business Model .....	
7.2 Prospective Market .....	
7.3 Acquisition of Customers .....	
7.4 Annual Costs .....	
7.5 Annual Profit and Return on Investment .....	
<b>8.0 Project Plan .....</b>	<b>93</b>
8.1 Work Breakdown Structure .....	
8.2 Schedule .....	
8.3 Critical Path .....	
8.4 Budget .....	
8.5 Earned Value Management .....	
8.6 Project Risks and Risk Mitigation .....	102

# 1.0 Context Analysis

## 1.1 Overview of Cable System

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 over 300 cable systems [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 cable systems can be over 3000 miles long.



*Worldwide submarine cable network [1] cable location data copyright PriMetrica*

Submarine cable systems come in many configurations; some are short and shallow connections that run a few hundred kilometers between neighboring countries, others run 10s of thousands of kilometers and connect dozens of countries together [1]. Of extra importance are the transoceanic cable systems that connect continents across the oceans. There are 53 such systems in place right now, with 31 new systems planned to be installed by year-end 2017 [13]. These systems are additionally important as they are may be the only connection between some smaller countries and islands. They are also the only connections available that can maintain the high-bandwidth required to run the modern global economy.

Name	Region	Length	Max depth	Bandwidth Capacity	Install Date
<b>FLAG Atlantic-1</b>	Transatlantic	14500 km	6000 m	2.4 Tbps	Jun 2001
<b>Tata TGN-Tata Indicom</b>	South Asian	3175 km	4500 m	5.12 Tbps	Nov 2003
<b>SEA-WE-ME-3</b>	Asian-Middle East-Europe	39000 km	6000 m	0.48 Tbps	Sep 1999
<b>Trans-Pacific Express</b>	Transpacific	17000 km	7000 m	5.12 Tbps	Aug 2008
<b>Middle East North Africa</b>	Middle East	8000 km	3000 m	5.7 Tbps	Dec 2014
<b>East Asia Crossing</b>	Pan East Asia	36500 km	9500 m	17.9 Tbps	Nov 2002
<b>GlobeNet</b>	N America - S America	23500 km	7500 m	1.36 Tbps	Oct 2000
<b>SEA-US</b>	Transpacific	15000 km	5000 m	20 Tbps	Q3 2016
<b>APX-East</b>	Transpacific	12500 km	6000 m	40 Tbps	Q4 2017

*Examples of the variety of cable systems [1]*

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]. Total investment in cables is significant, with \$11.8 billion invested from 2008 to 2014, and an additional \$4.8 billion invested in projects expected to be completed by 2017 [13].

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. The only protections are passive systems that are incapable of preventing some kinds of damage and cannot identify or deter harmful entities [10].

Damage also occurs 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].

## 1.2 Cable network as a bandwidth delivery service

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 343 cables consists of 2 major parts, regional cables and transoceanic cables [1]. Regional cables are relatively short systems that run between areas of one country, or in between neighboring countries. Data on these regional cables is relatively hard to come by, much of it is confidential, and there is no required data logging, or major studies on them.

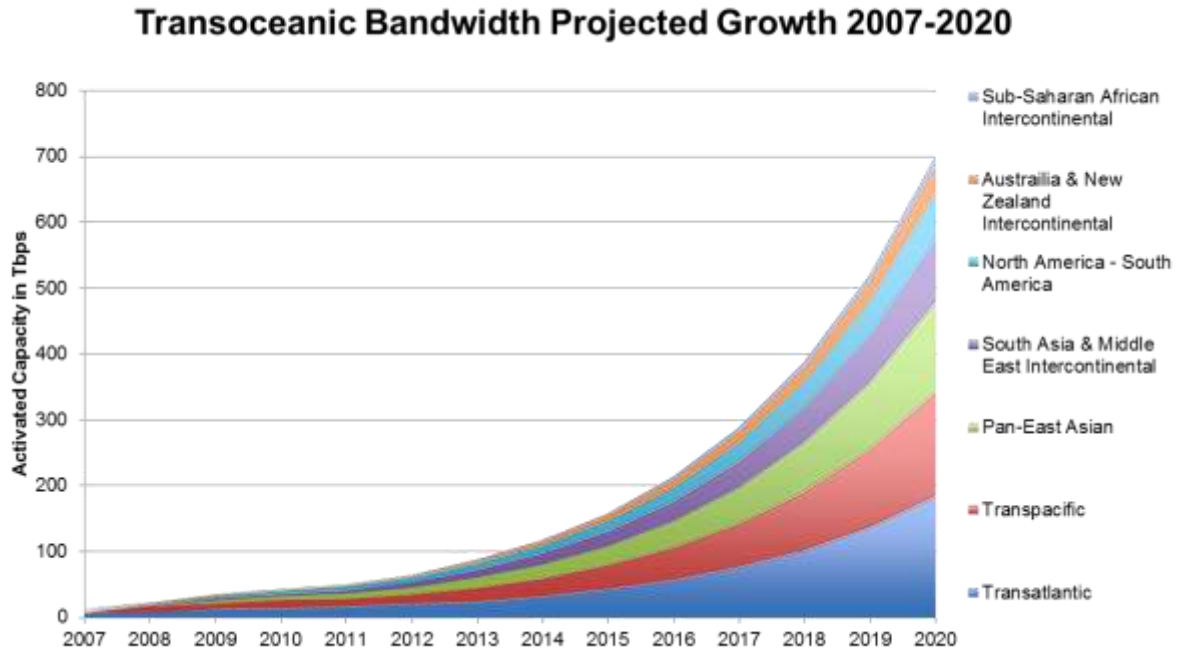
Significantly more data is available on the transoceanic cable system. This system can be divided into 7 major regions. These are the Transatlantic, Transpacific, Pan-east Asian, South Asia and Middle East Intercontinental, North and South American, Australia and New Zealand Intercontinental, and the Sub-Saharan African Intercontinental. The capabilities, growth, costs and threats vary significantly from region to region [13].

Route	Capacity (Tbps)	Growth Per Year (2007-2013)
Transatlantic	23	0.25
Transpacific	20	0.35
Pan-East Asian	17	0.46
South Asia & Middle East	12	0.42
North America-South America	9	0.52
Australia & New Zealand	5	0.4
Sub-Saharan African	2	0.57
Total Bandwidth	88	0.36

*Submarine Cable Capacity and Growth by Region [13]*

The Transatlantic is the oldest and most mature network, consisting of 9 systems, with a total capacity of 23 Tbps of bandwidth and average yearly growth of 25% over the last several years [13]. By contrast, the Sub-Saharan network is the least mature, with a total 1.8 Tbps capacity, but it has grown over 50% over the last 3 years, with many plans for additional bandwidth in the next few years [13].

The total transoceanic 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 5 years [13].



*Projected Transoceanic Bandwidth growth [13]*

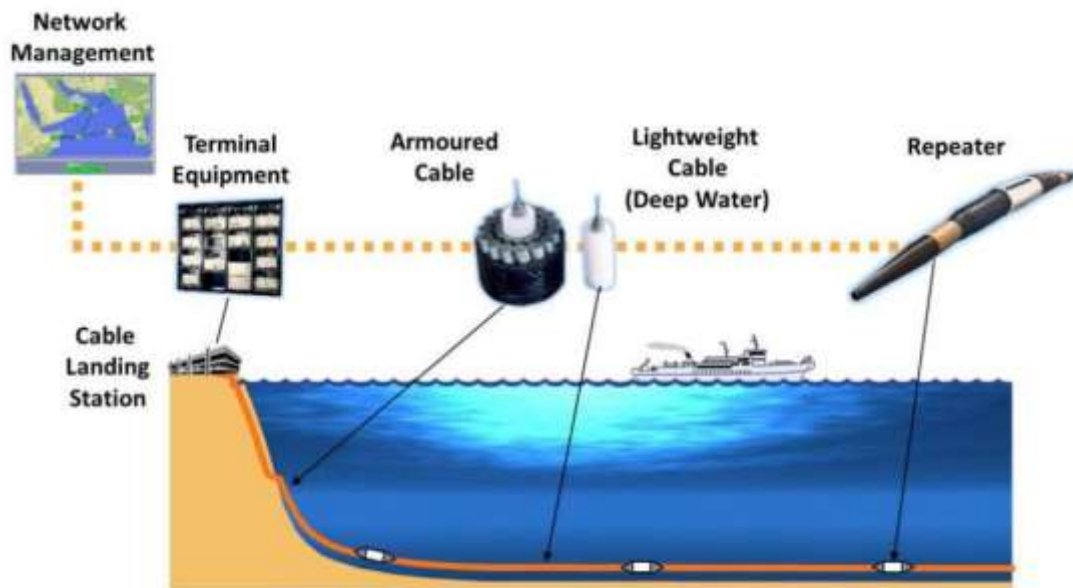
Bandwidth on these networks is rented out by the cable industry to land-based ISPs, other telecommunication industries, governments, technology companies and the finance industry. The standard rental unit used for pricing is 10 Gbps per month [14]. Prices vary from \$25,000 to \$250,000 per 10 Gbps per month, depending on the region and available bandwidth [6][14][15]. Individual technology companies are beginning to build their own personal cables to provide data services as well [9].

The bandwidth market expands to fill cable capacity rapidly as new cables are built. As such, there is little slack in the network to be taken up when cables are damaged and lose bandwidth. The available bandwidth of a new cable is typically completely sold before construction is completed and most cables are profitable within 5 years [6][8][9].

Organizations facing reduced bandwidth due cable faults can attempt to purchase bandwidth on other networks, but since little is available, a slowdown or complete loss of internet connection or other services is the most common outcome [10].

### 1.3 Cable construction and installation

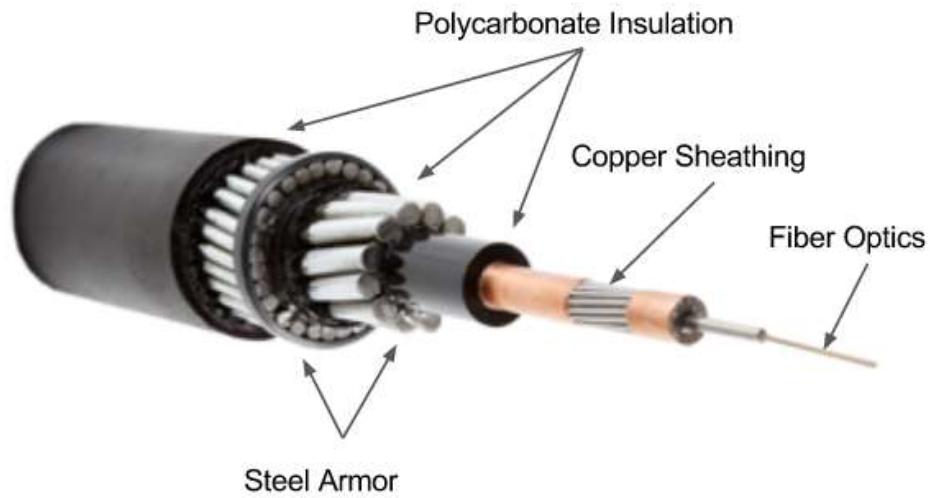
While cables can vary significantly depending on their technology, several basics span the industry. Systems have several major parts: cable landing stations (CLS), terminal equipment, fiber optic repeaters and the cables themselves. CLSs operate the terminal equipment to send and receive data [11]. These vary based on the cable technology and age.



*Typical Submarine Cable System [11]*

Data is transmitted via light pulses along glass fiber optics in the center of the cable. Around these fibers are a layer of petroleum insulation, a copper sheath and a final layer of polycarbonate insulation. This copper sheath carries 1 to 10 kilovolts of electricity to power the fiber optic repeaters. Repeaters are needed to amplify the light signals for distances over 100km, otherwise the signal is not strong enough to be receivable at the target CLS [10].

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



*A double-armored fiber optic cable [11]*

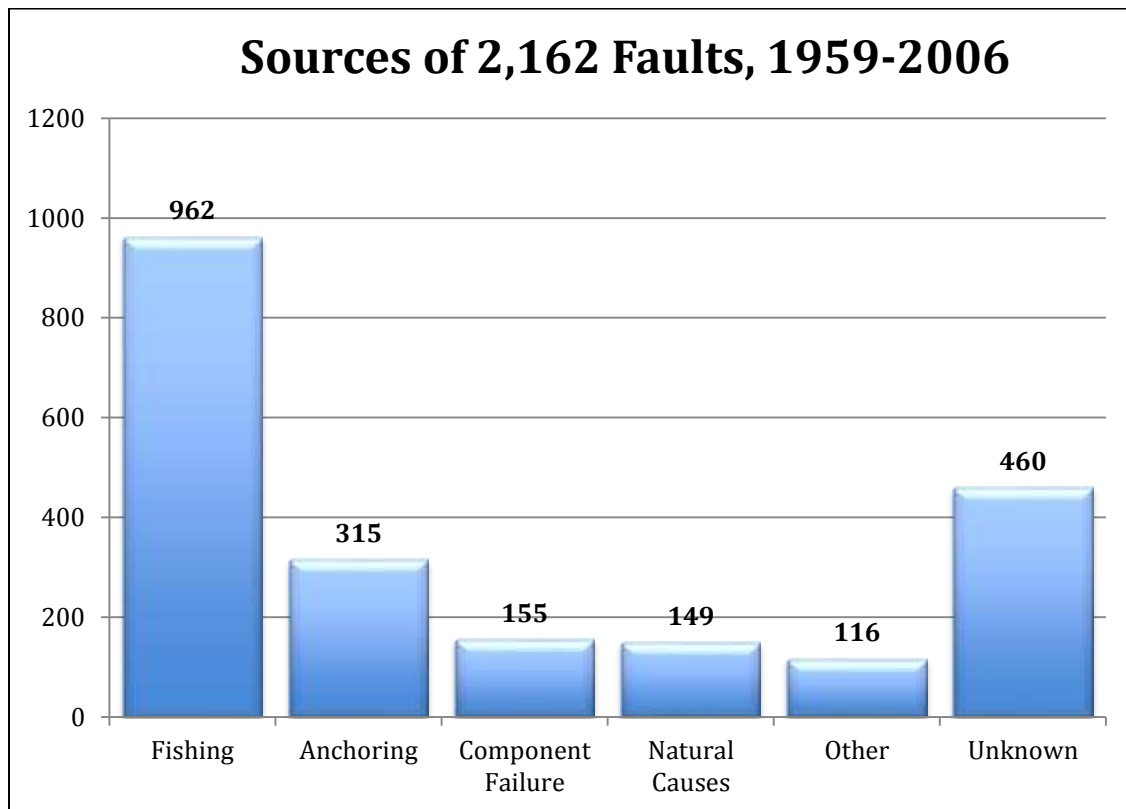


*Examples of different cable armor levels*

Cables in shallow waters are also buried a meter under the seabed where possible, again to protect them from damage. This is achieved by using sea ploughs or water jets to dig meter deep trenches into which the cable is buried. Burying cable is a slow process, typically progressing at a rate of 0.25 to 0.5km per hour [10]. This again adds significant cost and time delays to the installation process.

## 1.4 Threats and damage to cables

Cables are exposed to many threats and damage is frequent. Damage is divided into 2 large categories, external aggression faults and internal faults. External aggression is further decomposed into human and natural causes. Internal faults consist of component failures or installation errors and comprise approximately 7% of faults [10].



*Partial cable fault causes 1959-2006 [10]*

Natural external aggression incidents include earthquakes, animal attacks and abrasion incidents. Abrasion is caused by cables rubbing against hard or edged seafloor structures due to cable slack and ocean currents. Sonar is used during installation to lay cable avoiding such obstacles, but over time, abrasion of some degree is nearly inevitable. In all, natural external aggression makes up less than 7% of faults, with abrasion accounting for slightly over half [10].

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.

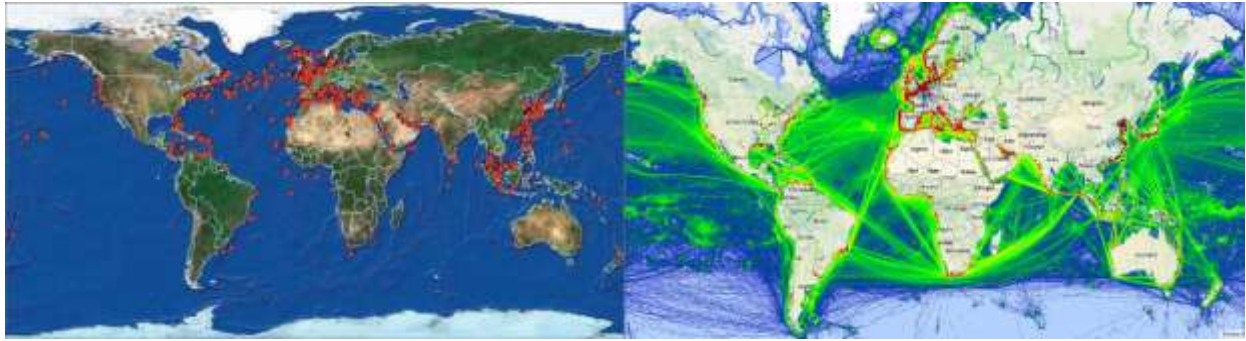
Damage from fishing is especially common, causing up to 44% of faults [10]. Trawl fishing is the largest culprit. While trawling, ships drag large nets with rigid edge structures along the seafloor. Unburied cables can be easily snagged by the trawl and subsequently lifted and broken by the ships. Even buried cables can be exposed over time, or dug up by these nets. The fishing equipment can be damaged or destroyed by this process along with the cable. There are even incidents of ships being capsized due to entanglement with armored cables [10].



*Beam trawler caught on submarine cable (red arrow) [10]*

Anchoring is another large cause of damage from human activity that is very difficult to protect the cables from. An average freight ship is approximately 6,000 tons without cargo and has two 5-ton anchors. When dropped, a 5 ton anchor can easily penetrate 5 meters into the seabed, and may be dragged for hundreds of meters through the seafloor as the ship comes to a stop [10]. Any cable in the way of such an anchor is destroyed or caught and entangled. 5 tons is actually a relatively small anchor – large ships equipping anchors up to 67 tons in weight are becoming more common.

Cable fault incidents due to commercial shipping and fishing activities are most common in regions with large interested in these industries. The seas around coastal Europe and southeast Asia have huge fishing and shipping industries and a similarly outsized number of cable fault incidents [10].



*Left: Cable Fault Incidents 1959-2006, Right: 2014 commercial ship traffic [10]*

While difficult to detect and prove, intentional human damage to cables is becoming an increasingly large threat. As cables are expensive and important infrastructure, they are a natural target for sabotage. There have been confirmed cases of intentional damage to cables in Egypt, Syria and Indonesia [2][3][4]. Faults in other regions have also been believed to be the result of sabotage [10].



*A frayed and severed cable, cause unknown [5]*

Submarine cables transmit nearly all international data; much of that data is sensitive and valuable making espionage of cables is an increasingly large threat. Espionage is very difficult to detect without direct surveillance, of which there is very little. A declassified 1970's era NSA program called Operation Ivy Bells was a coordinated and long term tapping of soviet subsea cables [21]. Information leaked recently by Edward Snowden indicates that current subsea cable espionage programs by the NSA or other foreign governments are likely and ongoing [20].

Recent Russian naval activity has also highlighted the vulnerability of the cable system to attack. The Russian military oceanographic ship *Yantar* was tracked through September and October of 2015 by the US Navy along the US east coast [33]. The ship seemed to be following cable paths and loitering around known cable installations. The ship is also equipped with 2 deep water remote submersibles [34]. Deep water cables (depths > 2000m) are generally considered protected due to their inaccessibility, but ships like the *Yantar* are easily capable of sending submersibles to those depths in order to sever cables or attach listening devices.



*The Russian Navy Yantar [33]*

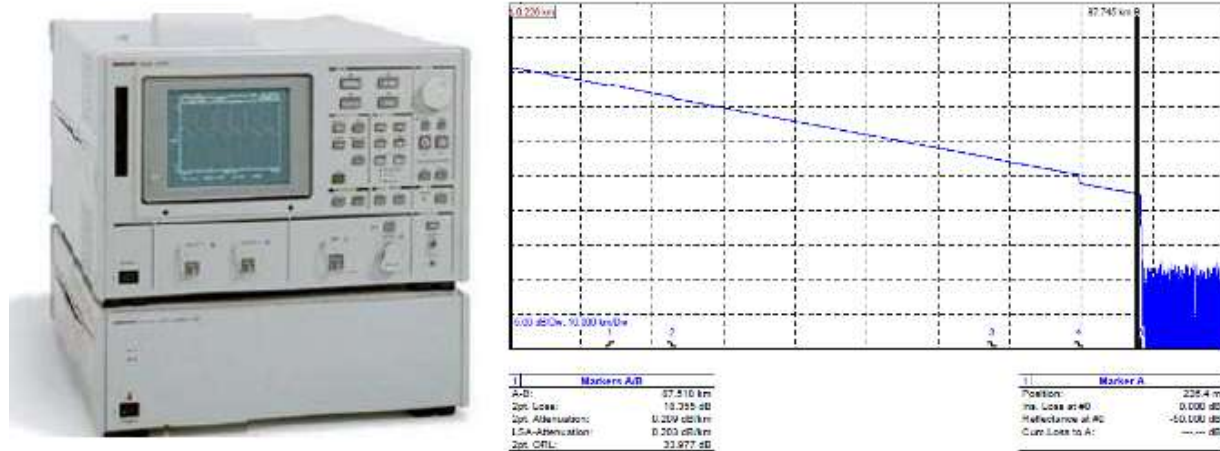
A major obstacle to reducing cable faults or preventing other problems is the lack of information. There is no global monitoring or reporting system in place, so analysis of cable faults is difficult. The FCC has recently acknowledged the size of the problem and has recently mandated new rules requiring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

## 1.5 Damage detection and location finding

There are 2 main types of faults experienced by submarine cables: shunt and optical faults. Both are largely detected immediately due to a loss of data transmission, but methods to locate the damage vary by the fault type.

Shunt faults are caused by the exposure to water of the copper electricity carrying sheath in the cable. Electricity is then shunted into the ocean, causing a failure of the fiber optic repeaters and degradation of data signals, regardless of any damage to the fiber optics. Power feed equipment (PFE) at the cable landing stations are used to locate the distance along the cable to within a few kilometers [10]. This is done by sending known voltages along the cable and measuring the resulting voltage drop to determine the distance from the CLS of the new ocean grounding point. This process is affected by many factors, including the earth's magnetic field and water temperature, making accurate measurements difficult.

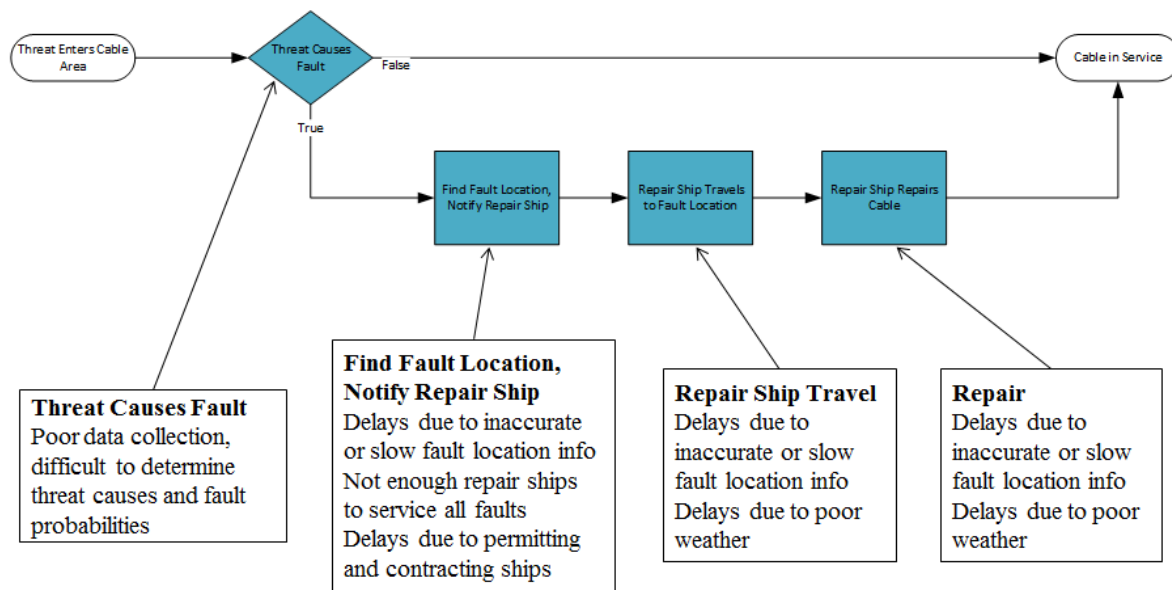
Optical faults are caused by damage to the fibers themselves by the crushing or severing of the cable. Optical faults can be located much more accurately than shunt faults with the use of specialized equipment. Optical Time Delay Refractometers (OTDRs) send a test pulse of known width down the fiber. Minute amounts of backscattering from the optical fault are measured to calculate the fault location. OTDRs cannot measure through repeaters though, so much more expensive and complicated Coherent Optical Time Delay Refractometers (COTDRs) are needed. These devices use additional fiber and the internal loopbacks of the repeaters to measure backscattering through the repeaters. Both OTDRs and COTDRs can determine optical fault locations to within 10 meters in a few minutes [29]. However these machines are expensive and not needed for normal functions, so very few CLSs have them.



*CODTR device and sample output*

## 1.6 Cable repair process

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].

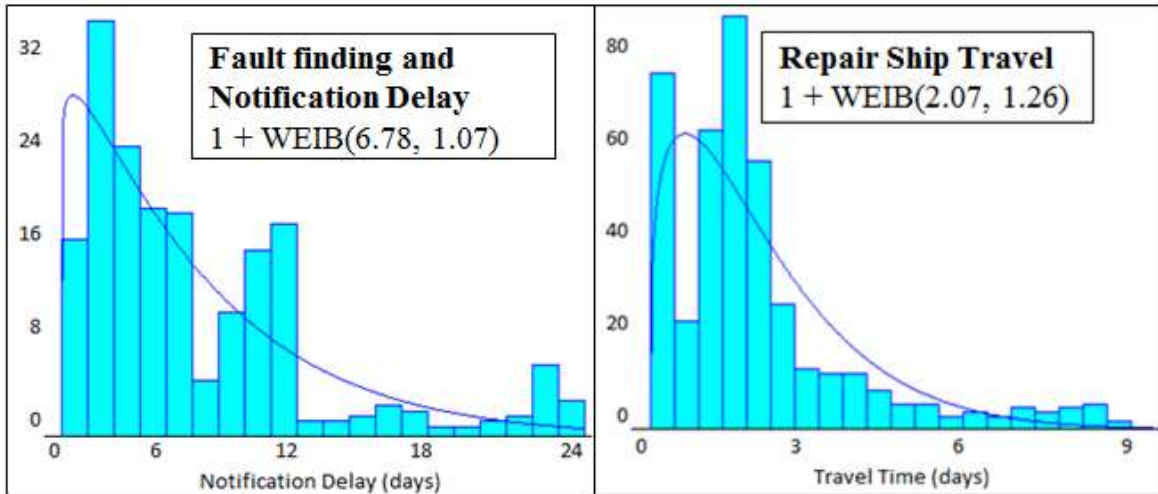


*Visualization of cable repair process*

There are 3 main delays in the repair process: fault location finding and repair ship notification, repair ship travel, and the repair itself.

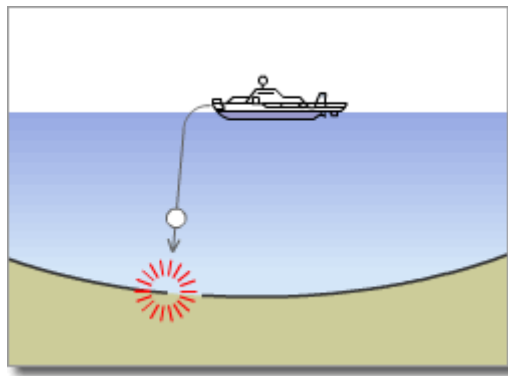
The fault finding and notification delay represents the time it takes to determine an accurate location of the fault, and to contract a repair ship for the job. Some cable companies own and operate their own repair ships, others must contract with a larger company, or individually owned repair ships when needed. There are approximately 60 cable ships in the world and most of the time, they are working on installing new cables or scheduled maintenance, making them unavailable for repair work [10][12][37]. Once contracted, the ship must then travel to the fault location to do the actual repair work.

In 2014, Telegeography published a study on repair delays of 456 cable faults from 40 originating countries [31]. We've fit distributions to this data:



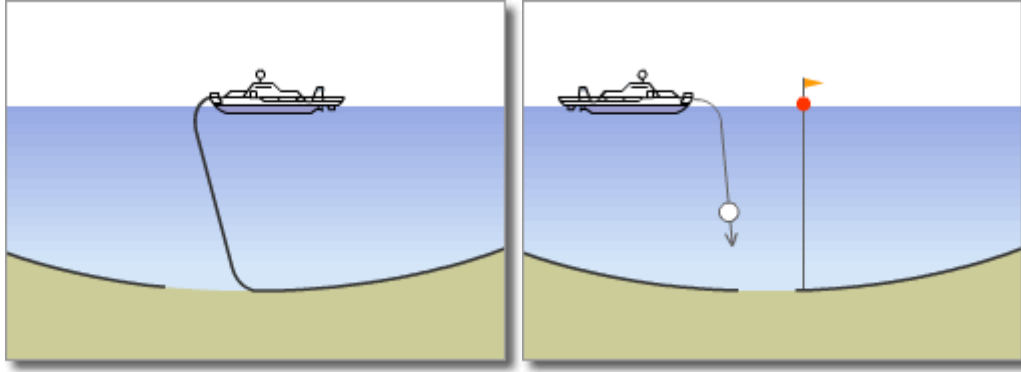
*Notification and Travel Delay [31]*

With the ship on site, the first step in the repair process is to retrieve the damaged cable from the seafloor. This is done dragging a special grapnel along the seabed that is designed to snag the cable and pull it to the surface. This process can be made faster by using a remote operated vehicle (ROV) to find the exact cable location, or can be done blindly making grapnel passes until the cable is found [18].



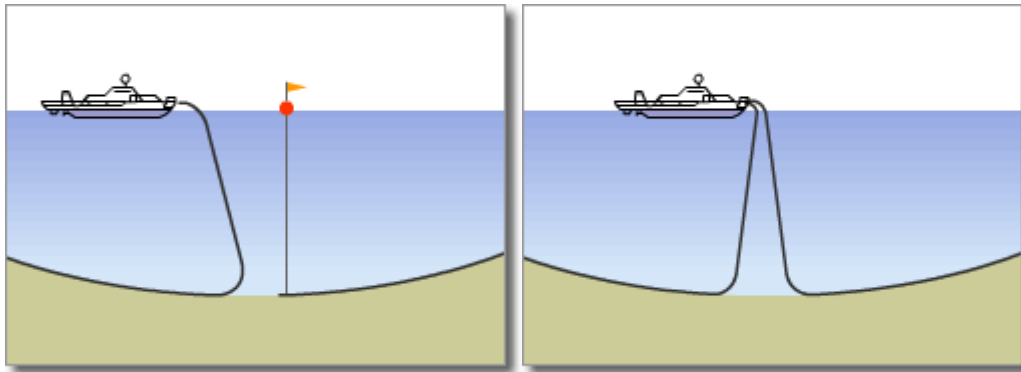
*Cable repair ship using a grapnel to find and retrieve severed cable [18]*

Next, the cable is severed if not already, and one end is brought on board. Dozens of meters of cable are cut off to remove any sections damaged by water ingress, then sealed. This end is then attached to a buoy and floated on the ocean surface [18].



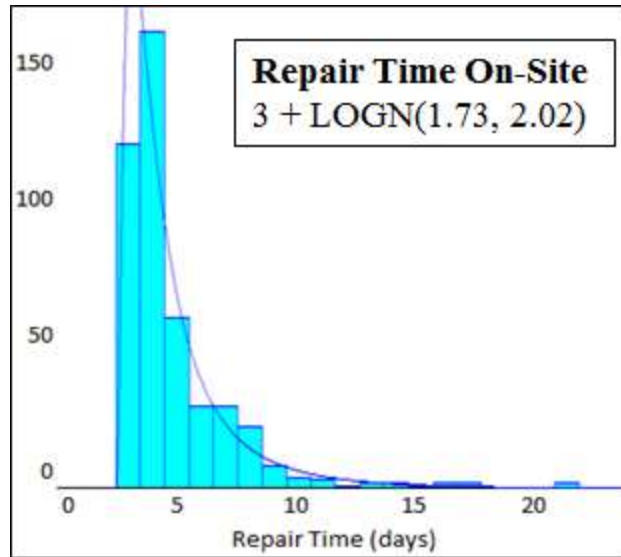
*Cable repair ship securing first cut end to a bouy [18]*

The other severed cable end is then brought on board the ship. Dozens of meters are again cut off due to water ingress. New sections of cable are then spliced onto the cut end and tested to ensure proper operation. The ship then sails back the buoy with the other sealed cable end. This end is unsealed and attached to the new section of cable. Once tested, the repaired cable is then lowered back to the seafloor [18].



*Cable repair ship reconnecting severed cable with new sections [18]*

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. Repair time for cables can be modeled by a lognormal distribution [38], and we have generated the following distribution to model this delay.



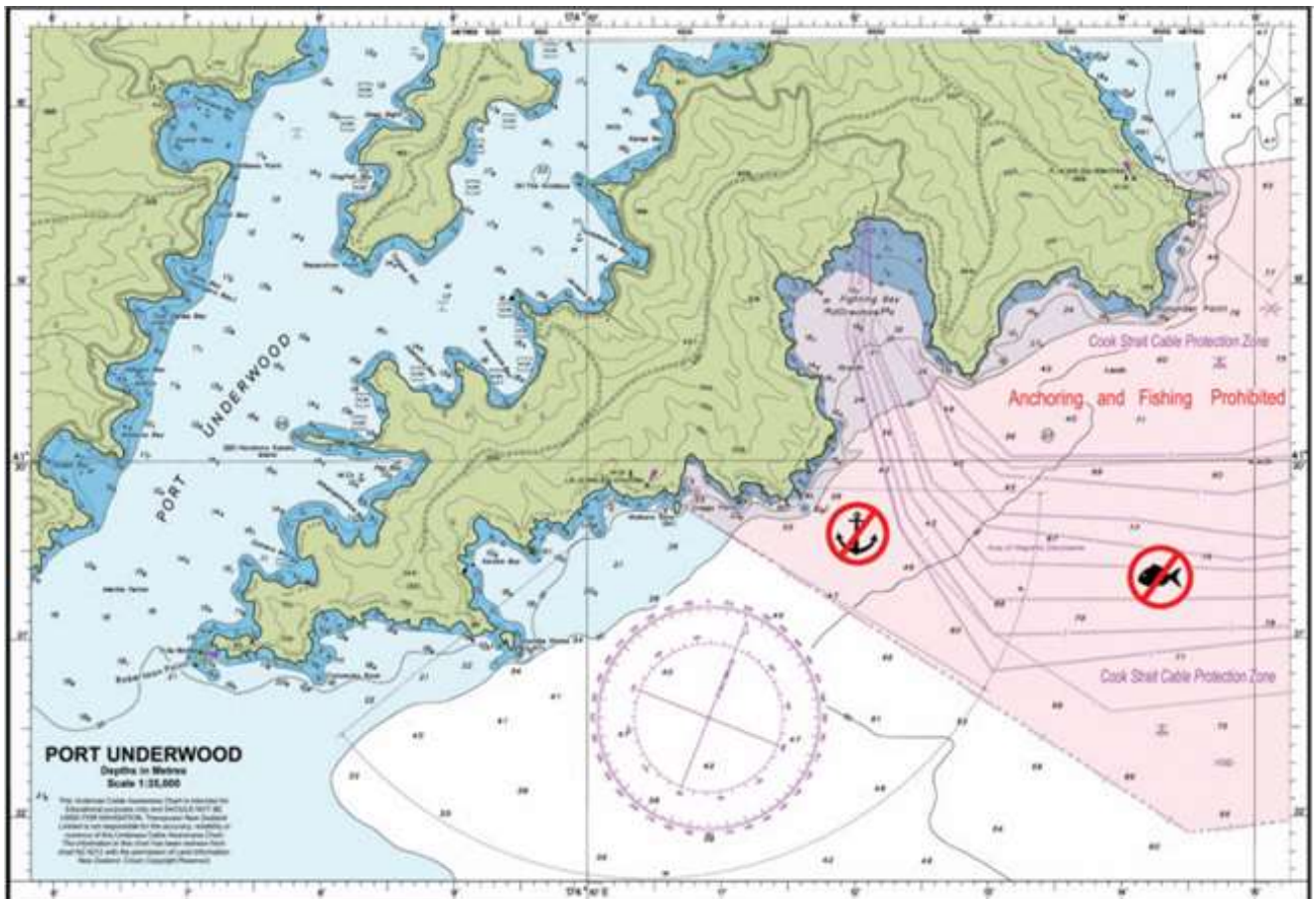
*Estimated distribution for repair delays*

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.

## 1.7 Cable protections

Since cables are valuable and critical infrastructure, there are organizations making efforts to protect them. The International Cable Protection Committee (ICPC) is the largest and oldest such organization. First established in 1958 in the UK as the Cable Damage Committee, it was renamed to the ICPC in 1967. The ICPC consists of representatives from telecommunications companies, governments and its own employees. It currently has 156 members from 60 different countries [19].

The ICPC has established best practices for companies to follow when installing, operating or repairing cables. It has also done significant research and published books, reports and informative presentations on all aspects of the submarine cable network [19]. It has also worked with governments to create cable protection zones to prevent cable damage and pursue legal action against companies or individuals who damage cables.



*Cable protection zone around Port Underwood, NZ [11]*

International treaties also exist between countries with significant investment in cable infrastructure. Treaties allow for provisions such as: special status for cable repair ships, sovereign cable zones up to 12 miles offshore of countries, criminal and civil penalties for damaging cables, fines up to \$300,000, obligations to prevent damage to existing cables when developing new underwater infrastructure and more [19].

However, these protections are only as good as their ability to be enforced, and the current lack of monitoring and surveillance of the cable system makes it very difficult to pursue legal action against cable damagers or even determine who is at fault. Approximately 20% of all cable faults never have a cause determined [10].

## 2.0 Stakeholder Analysis

### 2.1 Stakeholder Overview

For the purposes of this analysis, the stakeholder interactions are broken down into two different states: one, where the submarine cable system and associated stakeholders are presented as they are in the current system without modification; two, where they are presented as they would be with the introduction of the TCPS along with any new stakeholders. 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.

The following is a diagram depicting breakdown of the interactions among stakeholders within the current system. The submarine cable system is identified with a green rectangle. Similar stakeholders are grouped with generalized labels i.e. high bandwidth users, governments, maritime industry etc.

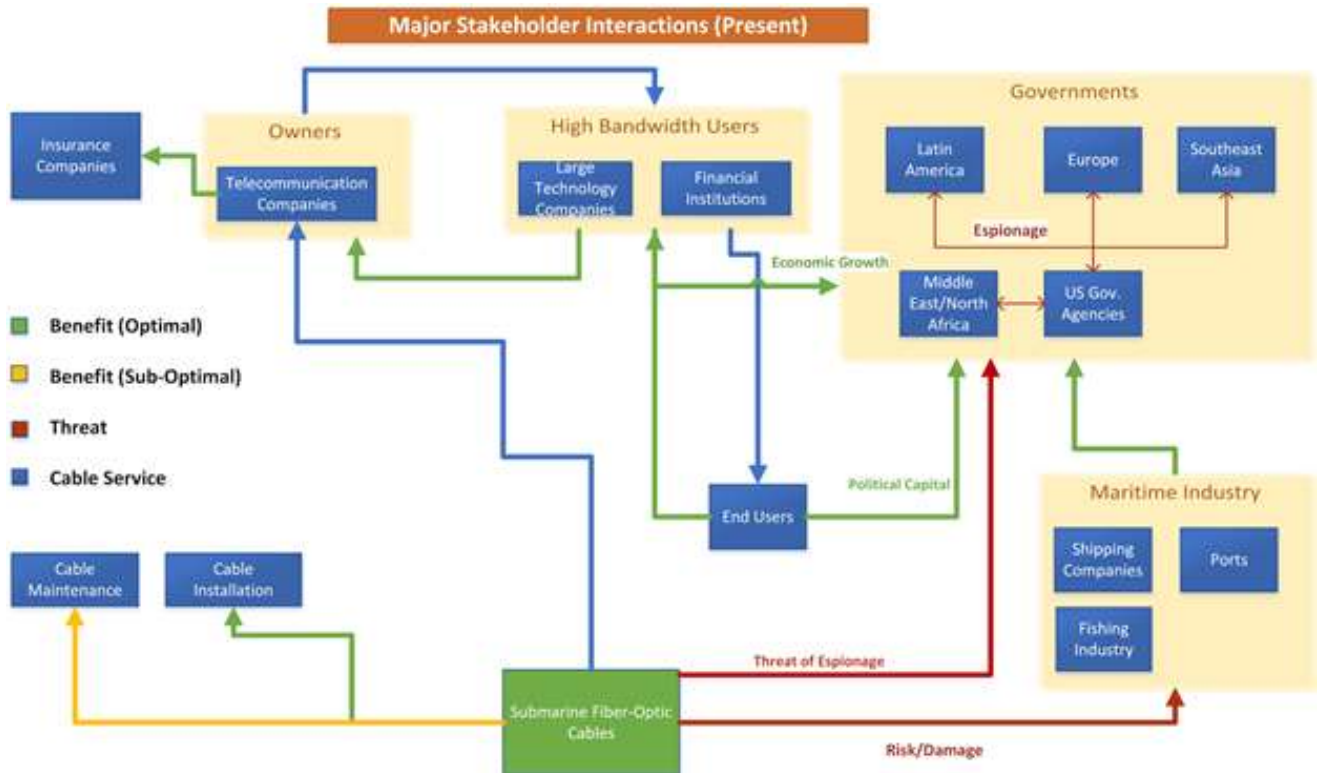


Figure 1. Stakeholder Interaction Diagram in present system

## 2.2 Primary Stakeholders

### *Direct Access Entities*

#### *Cable Installation and Maintenance*

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].  
Owners.

#### *Telecommunication Companies*

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].  
Maritime Industry

Over 60% of cable faults in regions in southeast Asia are the result of maritime vessels accidentally cutting fishing lines. Therefore, the objectives of the maritime industry are to reduce the damage associated with these accidental faults as prevent the faults in the first place.  
Governments

#### *U.S.*

Recent allegations of espionage have made cable security a priority [10]. Possible terrorist or intentional attack can put the infrastructure of the country at risk, therefore, protecting the cables is a military imperative [13].

### *South America*

In order to prevent foreign countries from spying on Latin American communication, major pushes have been made to implement a direct line between Europe and South America [13].

### *Europe*

Similar to the United States, Europe is concerned with the security of the information passing through their communication lines. As a result, there has been significant political momentum towards securing the cables lines from unwanted tapping [13].

### *Middle East*

Recent accounts of terrorist activity have led to the damage of submarine cables. However, in contrast to the other geopolitical regions, the middle east is more concerned with the jurisdiction of a cable security system as it would apply to interactional oversight. There is strong preference for a decentralized system[13].

## **2.3 Secondary Stakeholders**

### *Insurance Companies*

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.

### *High Bandwidth Users*

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.

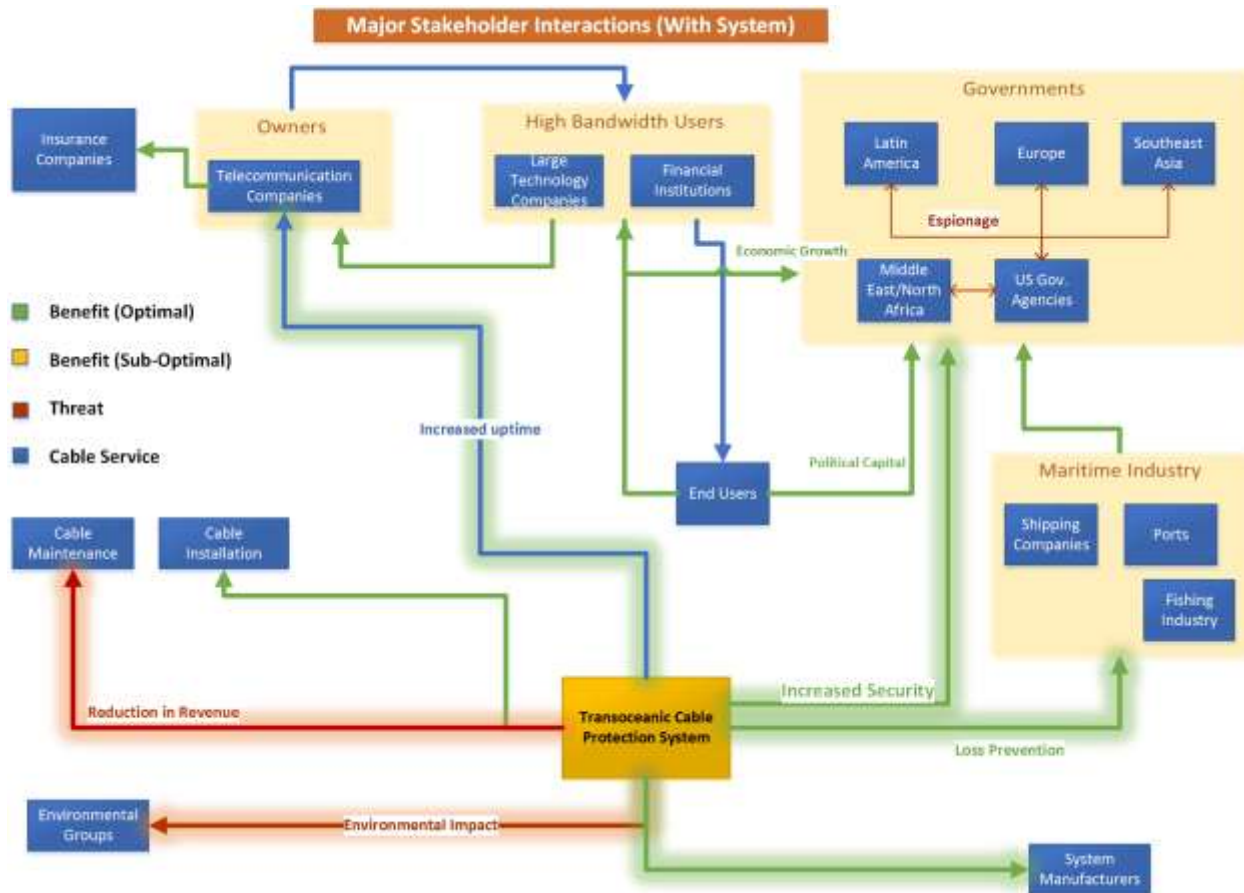


Figure 2. Stakeholder Interaction Diagram post implementation of TCPS

The following table shows the positive changes that occur between stakeholders between the current system and the TCPS.

### Positive Changes

Entity	Current System	With System
Owners	Low Reliability	Increased Uptime
Governments	Threat of Espionage	Increased Security
Maritime Industry	Vessel Damage/Litigation	Prevention/Clarity
System Manufacturers	No Market	Increased Revenue

The following table shows the negative changes that occur as a result of the implementation of the TCPS along with possible solutions for ensuring a win-win situation

### Negative Changes

<b>Entity</b>	<b>Problem</b>	<b>Solution</b>
Repair Companies	Reduced Revenue	Shift Resources from Repair to Monitoring
Environmental Groups	Disruption of Ecosystem	Extensive Testing/Minimal invasiveness

## **3.0 Problem and Need**

### **3.1 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 150 cable faults occur every year. Around 60% are caused by accidental causes such as anchor drops and fishing incidents. Meanwhile, 20% of faults are caused by unknown causes. However, there are increasing fears of sabotage and espionage by malicious groups due to a few reported incidents. In addition, the ability to detect and repair faults is slow and costly, with an average of 3 weeks of down time for repair and about \$3 million lost for each cable.

### **3.2 Statement of Need**

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 system 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.

### **3.3 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.

Perhaps a more serious risk involved with underwater cables is the threat of wire-tapping and intentional wire cuts [21]. Wire taps from spies and other agencies could be devastating to a

government if sensitive or classified information was to be stolen. There is currently no constant monitoring of these cables, which presents a major performance gap. There is an obvious need to protect this critical infrastructure, especially in today's world where so much data travels through these cables.

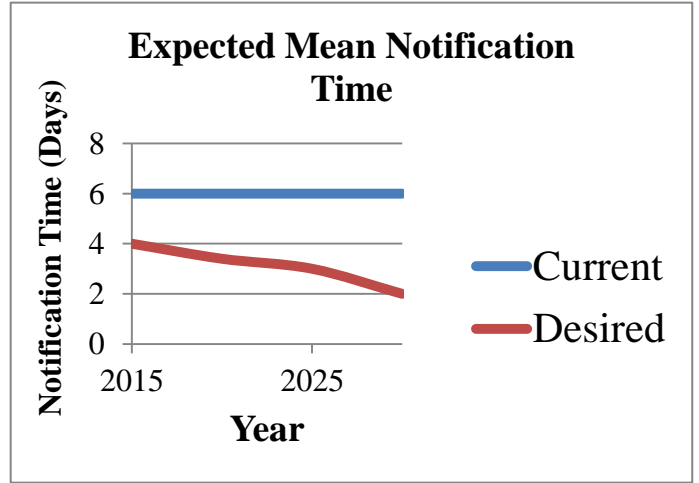
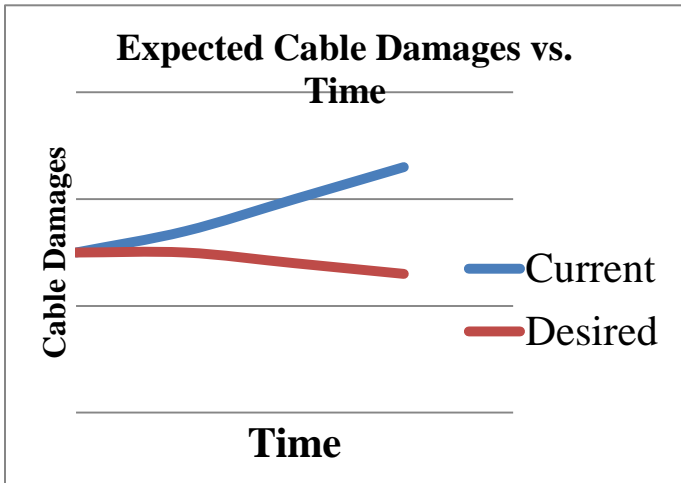
Developing a process to ensure protection of these cables is the purpose of the Transoceanic Cable Protection System. Total protection of the cables may be infeasible due to the vastness of the oceans and the depths they reach. However, with a proper system alternative, the aim is to reduce cable damages by 30% each year. This will be done through better surveillance and most importantly, better communication to deter threats. For example, if the solution system is able to notify a ship that it is near a cable and instruct it not to drop anchor in the area, then it would be considered a success. If a fishing boat is trawling and coming within reach of a cable, the system would notify the fisherman to lift his nets in order to avoid hitting the cable. This is a "win-win" scenario because both parties are not interested in damaging the cables or their own equipment (anchors, fishing nets). Defending against terrorist attacks or wire-tapping will be a much more difficult task. It is assumed that these spies and/or terrorists will be trained divers operating in secret. Notifying the diver that he is near a cable would defeat the purpose of the surveillance system. In this case, our system would have to be able to notify appropriate authorities, such as military or security agencies, that there is a potential attack occurring at a specific location. Our system itself must be covert, with the intention of making covert actors overt. Once notified, these authorities would take necessary action. The system would also have to differentiate between sea animals and divers, which is another potential risk. Reducing the cable damages by 30% each year will automatically save cable owners money by reducing repair costs and increasing cable uptime.

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.

The last major performance gap that we have identified is the notification time of a cable fault. Our system seeks to reduce the mean notification time by two days. Doing so will help reduce cable downtime by organizing the repair process and making it easier for cable repair companies to do their job.

Closing this gap will be no easy task. Our team will be analyzing multiple alternatives to determine which type of system will be most effective in meeting the requirements. Mission, functional and design requirements will be discussed in the following sections. The following

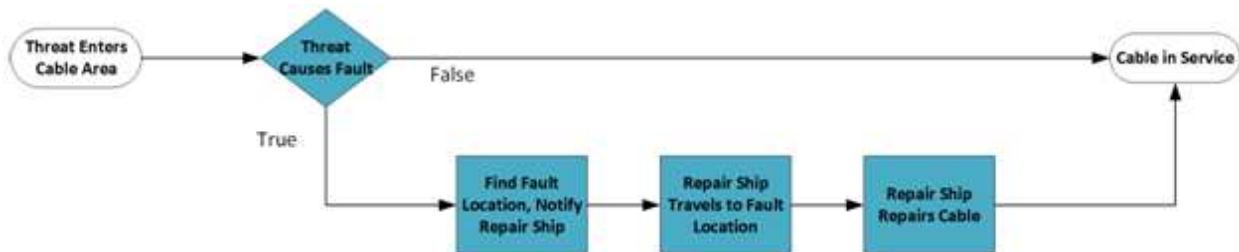
graphs show a trend in what we expect with the current state of the system and our desired outcome with TCPS. With more cables being laid over the next several years, we expect more cable damages to occur, which is shown in the trend. The graph on the right shows the current mean notification times and the desired level with our system.



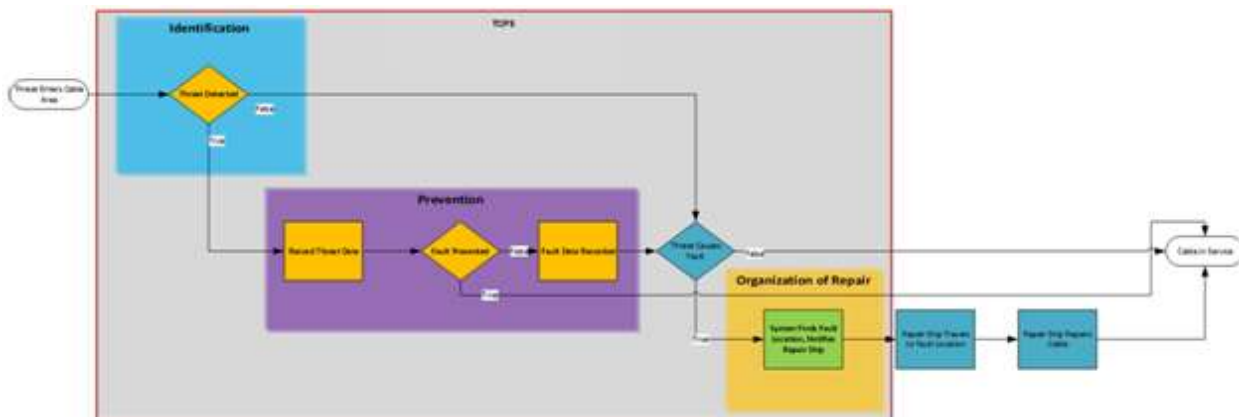
## 4.0 Operational Concept

The proposed solution is the Transoceanic Cable Protection System (TCPS). The TCPS will have three functions: (1) Threat Identification, (2) Prevention, and (3) Repair Coordination. The basic procedure of the system starts with identifying and detecting threats. Once a threat is detected, prevention efforts are initiated. If damage does occur, the next objective is to reduce cable downtime by coordinating repair.

The diagram below shows the current process of the cable system. First, a threat enters a cable area. The threat either causes the fault or it does not cause the fault. If the threat does not cause a fault, the cable continues its service.. In the event that a threat causes a fault, three processes occur. First, the cable owner attempts to locate the cable fault and contacts a repair ship. Delays can occur during this process due to slow acquisition of fault location information. The number of repair ships is also limited. Plus, delays can occur due to permitting and contracting ships. Second, the repair ship must travel to the fault location. This process 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, which results with the cable being back in service. Delays during this last process can occur due to inaccurate fault information and poor weather.



The next diagram shows where our system will be implemented in the current system. Each function will operate in its respective area. Following the entrance of a threat in the cable system, Threat Identification begins. It is then followed by the Prevention function. Finally, Repair Coordination function will begin in the event that the system is unable to prevent damage.



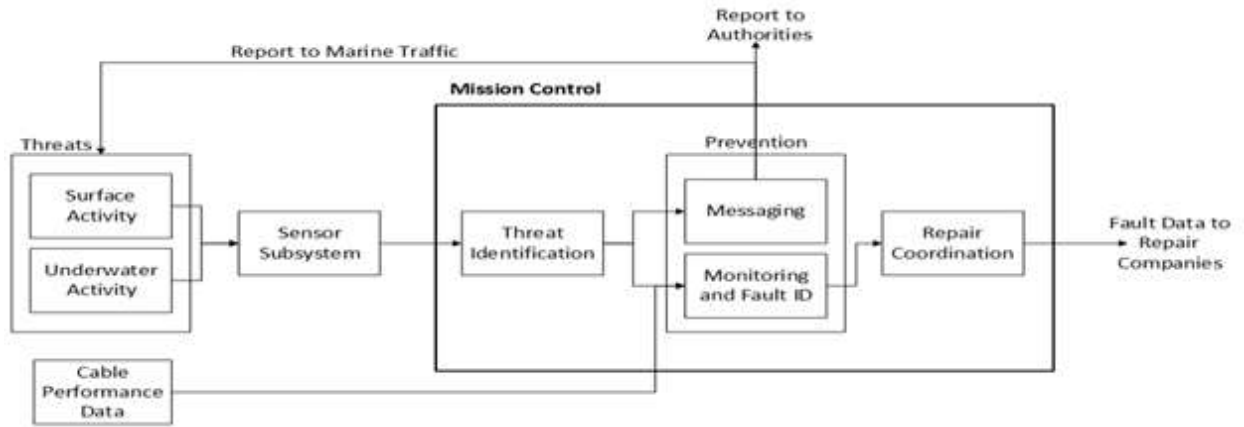
Threat Identification is the first step to preventing cable damage from occurring. Within this function, the system will identify three things: surface-level threats and underwater threats,. As mentioned

in the Problem Statement, 20% of the threats that cause cable damages are unknown. Identifying surface-level threats, such as shipping and fishing vessels, will be possible using surface-level surveillance.. Identifying underwater threats, such as saboteurs or espionage devices, will be much more difficult to detect because the ocean is expansive and the technology to perform underwater monitoring is limited. The method through which TCPS will accomplish this task will be discussed in the design alternatives.

Prevention is the second function of TCPS. It will stem from two aspects: forecasting and communication. Based on research, 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, it can be forecasted that it is more likely for cable faults to happen in this area. 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 ships of their proximity to cable areas and instructing them to refrain from trawling or dropping anchor in particular areas can potentially reduce cable faults. With regards to the intentional human action, TCPS 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 function depends on the results of the identification function.

Repair Coordination is the third function of the TCPS. The current process is slow and costly, and the TCPS will aim to reduce the downtime and cost of repair. The system will organize repair process by notifying repair companies of the fault type and location of the fault. This will reduce the amount of time spent searching for the section of the cable that is damaged. Just as with the prevention operation, this operation will also depend on the proper identification of fault location and type of fault.

The entire solution encompasses the need to perform these functions from a central location. Thus, all aforementioned functions will be centralized in 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 from the Identification alternatives. Using this data, the system will identify threats to the cables. Prevention of damage will occur using the information gathered on threats. Prevention will be facilitated 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 Repair Coordination, 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 the diagram below.



## 5.0 Requirements

Requirements for the TCPS were derived from a need stated by our sponsor, which is to survey and monitor underwater infrastructures. We have developed these requirements through research on undersea cables and the previous fault data. Any assumptions that we have made will be explained in the requirements. We first created high-level Mission Requirements, which explain what TCPS will do. From these, Functional and Design Requirements were developed to describe how TCPS would meet the Mission Requirements.

### 5.1 Mission Requirements

- MR 1.0: TCPS shall monitor cables 24 hours per day.
  - MR 1.1: The system shall be capable of monitoring at least 50% of the total cable length.
  - MR 1.1: The system shall be able to monitor at least 50% of littoral zones.
- MR 2.0: TCPS shall provide real-time threat information to appropriate authorities.
- MR 3.0: TCPS shall detect fault location to within 100 meters.
  - MR 3.1: The system shall provide fault information to cable owner and repair companies within one hour.

These requirements describe what TCPS should be able to do. From the Concept of Operations section, we identified that our system will 1) Identify Threats, 2) Prevent faults and monitor cables, and 3) Coordinate the repair process. These Mission Requirements will serve as the verification measure for TCPS.

### 5.2 Functional Requirements

- FR 1.0: Monitoring and Surveillance of Cables: The system shall monitor and survey cables and cable zones.
  - FR 1.1 System Coverage
    - *FR 1.1.1 Depth*: The system shall be able to operate at depths greater than 3,500 meters below the surface level.
    - *FR 1.1.2 Width Coverage*: The system shall detect threats within 100 meters of either side of the cable.
    - *FR 1.1.3 Height Coverage*: The system shall be able to monitor the cable from at least 200 meters above the cable.
    - *FR 1.1.4 Location*: The system shall be located within 50 meters of either side of the cable.
    - *FR 1.1.5 Cable Coverage*: The system shall be able to survey at least 80% of the cable length.
  - FR 1.2 Maintenance

- *FR 1.2.1 System Uptime:* The system shall have at least a 95% uptime.
  - *FR 1.2.2 Operating Time:* The system shall be capable of operating for 60 consecutive days.
  - *FR 1.2.3 Repair:* The system shall be able to be repaired on-site.
  - *FR 1.2.4 Repair Remotely:* The system components may be able to be repaired remotely.
- FR 2.0: Identification of Threats: The system shall identify threats.
  - FR 2.1 Information Gathering: The system shall gather information about the surface area.
  - FR 2.2 Aggregate Information: The system shall aggregate collected information to determine safety of cables.
  - FR 2.3 Interpret Information: The system shall require system operators to interpret information.
    - *FR 2.3.1 View information:* The system shall allow the operator to view the information on a visual display.
    - *FR 2.3.2 Analyze information:* The system shall allow the operator to analyze the information for threats.
- FR 3.0: Find Cable Damages: The COTDR shall identify fault location to within 100 meters.
- FR 4.0: Communication with Outside Stakeholders: The system shall allow communication with outside stakeholders.
  - FR 4.1 Receive Communication: The system shall be able receive pre-defined encrypted communication from outside stakeholders.
    - *FR 4.1.1 Self-Status Requests:* The system shall be able to receive self-status update requests.
    - *FR 4.1.2 Monitoring Status Request:* The system shall be able to receive monitoring-status update requests.
    - *FR 4.1.3 Potential Threat Parameters:* The system shall be able to receive potential threat parameters.
    - *FR 4.1.4 Marine Vessel:* The system shall be able to receive communication from marine vessels in the area of operation.
  - FR 4.2 Send Communication
    - *FR 4.2.1 Self-Status Updates:* The system shall be able to send self-status updates periodically and upon request.
    - *FR 4.2.2 Monitoring Status Updates:* The system shall be able to send monitoring -status updates periodically and upon request.
    - *FR 4.2.3 Threat Parameter Updates:* The system shall be able to send threat parameters updates periodically and upon request
- FR 5.0: Monitoring and Security of System: The system shall perform self-monitoring to ensure safety of system.

### 5.3 Design Requirements

The current Design Requirements are not for a specific system. Due to the variety of alternatives, which will be discussed in the next section, different designs will be needed for

TCPS. Our final Design Requirements will be specific for each alternative. The following Design Requirements are for a general TCPS and further explain how the system will meet the Mission Requirements.

- DR 1.0 The system shall have an above water subsystem.
  - DR 1.1: The system shall have servers that manage all collected data integrally.
  - DR 1.2: The system shall have data processing technologies.
  - DR 1.3: The system shall display the data to the operator.
  - DR 1.4: The system shall have communication equipment.
  - DR 1.5: The system shall have a power supply for the underwater subsystem.
- DR 2.0: The system may have an underwater subsystem.
  - DR 2.1: The system shall have communications equipment for exchanging information with the above water subsystem.
  - DR 2.2: The system shall have threat detection technology.
    - DR 2.2.1: The system shall have sonar or acoustic sensor technology.
    - DR 2.2.2: The system shall have a platform for sonar sensor technology.

## **6.0 Design Alternatives**

Because the system will be monitoring underwater cables, we are limited with technology that will accomplish the task. Just as air traffic controllers use radar to track aircraft traveling through airspace, our system will also rely on signals to track and identify threats. Monitoring activity underwater and detecting objects is a major challenge. First, light and radar waves do not propagate well through water. This limits a system's ability to see and detect surrounding objects. This leaves us with sonar sensors as our only option while under water. Sonar systems have evolved over the years and can produce high-resolution images of surrounding objects. Sonar is broken down into two categories, active and passive. Current sonar systems have been researched and analyzed in order to determine the most effective means of monitoring underwater cables.

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.

### **6.1 Surface Threat Identification Alternative**

At least 60% of cable faults are caused by commercial shipping and fishing activities [10]. Because it can take days to determine the fault location, it is difficult to identify which ship may have caused the damage. Since ships are liable for fines and damage it is in TCPS interest to be able to determine ships responsible for damage faster and with better accuracy.

Cable protection zones are not universal and do not cover entire lengths of cable where they do exist. Better communication with ships that are unaware cables are in their area may be able to prevent some cable fault incidents.

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.

Of course, these alternatives cannot monitor underwater threats. They are envisioned as low cost, high potential return additions to other system alternatives. Depending on the region

and stakeholder, they may also meet stakeholder needs at a fraction of the cost of the complete system.

### ***6.1.1 Automatic Identification System***

Automatic Identification System (AIS) transponders are required equipment on all vessels over 299 tons. These devices relay a ship's 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].

### ***6.1.2 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].

## **6.2 Underwater Threat Identification Alternatives**

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 Buoy. These platforms will allow the platforms to record data and maneuver through the water.

### ***6.2.1 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. Signals can be emitted at various frequencies, which will produce images of differing resolutions. 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.

#### ***6.2.1.1 Synthetic Aperture Sonar***

Synthetic Aperture Sonar (SAS) is a relatively new technology that is widely used in support of any job that requires surveying. These jobs include offshore oil and drilling inspection, seafloor imaging, and search and recovery missions [23]. SAS provides very high-resolution images (up to 10 times higher than Side Scan and Multibeam sonar) 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. Sonar technology prior to SAS required two separate systems to get topographical maps and bathymetry information [23].

SAS operates by emitting sound energy in the shape of a fan towards the desired target. Along with this, SAS sends consecutive “pings” with the sound energy, which calculates the depth. SAS can be integrated with Autonomous Undersea Vehicles (AUV) and Remote Operated Vehicles (ROV). Below is a specifications table, which will show if SAS meets our requirements.

<b>Type</b>	Active	<b>Signal Properties</b>	
<b>Depth Rating</b>	6,000 m	<b>Frequency</b>	175 kHz
<b>Signal Range</b>	300 m	<b>Pulse Length</b>	1, 5, or 10 $\mu$ s
<b>Wide-Scan Range</b>	250 m each side	<b>Number of Beams</b>	14 (7 port, 7 starboard)
<b>Operating Speed</b>	4-1,010 knots	<b>Array Length</b>	1.36 m
<b>Coverage</b>	3 km <sup>2</sup> /hr	<b>Power</b>	110/240 V AC
<b>Resolution</b>	3 cm	<b>Inertial Navigation System</b>	Yes
<b>Real time processing</b>	Yes	<b>Memory</b>	16 GB RAM

### 6.2.1.2 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. This allows CHIRP to produce images up to 5 times the resolution of side scan and multibeam sonar without worrying about irregularities of fast moving objects like fish or divers.

The table below lists the specifications for CHIRP. One benefit of this technology is that it has a high and low frequency setting, which allows the user to trade-off between longer signal range or better image resolution. CHIRP is also able to be integrated on AUVs, ROVs and aboard ships [23].

<b>Type</b>	Active	<b>Signal Properties</b>	
<b>Depth Range</b>	6,800 m	<b>Frequency</b>	650 kHz (High), 325 kHz (Low)
<b>Signal Range</b>	300 m (Low), 100 m (High)	<b>Pulse Length</b>	200 $\mu$ s (High), 400 $\mu$ s (Low)
<b>Wide-Scan Range</b>	200 m each side	<b>Source Level</b>	210 dB at 1 $\mu$ Pa at 1 m
<b>Operating Speed</b>	Not Available	<b>Array Length</b>	Not Available
<b>Coverage</b>	360° Capability	<b>Power</b>	20-36 V DC
<b>Resolution</b>	15 mm	<b>Inertial Navigation System</b>	No
<b>Real time processing</b>	Yes	<b>Memory/Processing</b>	156 kbits/s

### 6.2.1.3 Side-scan and Multibeam Sonar

Side-scan and Multibeam (SSM) 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. It is capable of imaging, but it covers a significantly smaller area than side-scan. When integrating these two sonars, one can obtain both topographical and bathymetric information. SSM is compatible with ROV, AUV, and is generally towed behind ships [23].

<b>Type</b>	Active	<b>Signal Properties</b>	
<b>Depth Range</b>	4,000 m	<b>Frequency</b>	150-1800 kHz
<b>Signal Range</b>	15-400 m	<b>Pulse Length</b>	4.44-27 $\mu$ s (High to Low Frequency)
<b>Wide-Scan Range</b>	100 m	<b>Source Level</b>	Not Available
<b>Operating Speed</b>	5.38 knots	<b>Array Length</b>	Not Available
<b>Coverage</b>	~180° Capability	<b>Power</b>	< 10 V DC
<b>Resolution</b>	5 cm at 1800 kHz, 30.5 cm at 150 kHz	<b>Inertial Navigation System</b>	No
<b>Real time processing?</b>	Yes	<b>Memory/Processing</b>	Dependent on processor

### 6.2.2 Passive Sonar Alternative

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. The following alternative could provide detailed information for the surveillance and security of undersea cables.

#### 6.2.2.1 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. It is a very versatile technology, being able to be mounted on ROV, AUV or in an acoustic array of nodes. Acoustic arrays are networks of hydrophones that operate by using triangulation to detect and locate threats. This is done through various methods, including Long Baseline Localization or Short Baseline Localization. Hydrophones can have a listening radius up to 16 kilometers. A drawback of hydrophones is that they cannot produce images of surrounding images like active sonars can. However, noise created by objects such as engines or animals have specific frequencies, allowing a hydrophone to differentiate between threats and non-threats. The following table lists the specifications of hydrophones [26].

<b>Type</b>	Passive	<b>Frequency</b>	46 kHz
<b>Depth Range</b>	3,500 m	<b>Voltage</b>	12-30 V DC
<b>Receive Sensitivity</b>	204 dB re 1 V/ $\mu$ pa	<b>Current</b>	10 mA
<b>Horizontal Directivity</b>	1 dB to 40 kHz	<b>Preamplifier gain</b>	37 dB
<b>Vertical Directivity</b>	1 dB to 20 kHz	<b>Operating temperature</b>	0-55°C
<b>Real time processing</b>	Yes	<b>Listening Range</b>	1-15,000 Hz

### **6.2.3 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 Hydrophone Array Buoys. Decision criteria will be based on cost, effectiveness, and capabilities. While there are many AUVs and ROVs on the market that could potentially satisfy our requirements, we will analyze various platforms with different capabilities.

#### **6.2.3.1 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. To survey a cable across the Atlantic Ocean, it could potentially cost millions of dollars due to the speed at which they must travel. Strong currents can also pose a threat to the safety of the ROV [27]. To mitigate the risk of damage to the ROV from ocean currents and other factors, ROVs are equipped with propulsion systems, allowing them to move in any direction.

Three ROVs will potentially be used as platforms: ASI Mohican, Oceaneering NEXXUS, and Oceaneering Millennium Plus. After analyzing the utility of ROVs in TCPS, it was determined that ROVs would not be useful in the threat identification and prevention functions. There could be a potential use for finding and repairing specific cable fault locations.

##### **6.2.3.1.1 ASI Mohican ROV**

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].

##### **6.2.3.1.2 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].

##### **6.2.3.1.3 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.

### 6.2.3.2 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. AUVs can be diesel powered or lithium battery powered, which is used to propel the vehicle forward. AUVs can also be controlled manually or programmed with a predetermined route.

There are benefits and drawbacks of employing an AUV. Several benefits include operation in very deep water, programmable routes and versatility. Drawbacks include potentially slow communication between the AUV and outside stakeholders, hazardous terrain, slow traveling speeds (0.25-2 m/s), and short battery life. Though an AUV could potentially survey the entire length of a cable, it would take a very long period of time. Thus, multiple AUVs would need to be deployed to provide constant surveillance. For an AUV capable of traveling at 1 m/s, it would take roughly 1,400 hours (58 days) to travel 5,000 kilometers (about the length across the Atlantic Ocean from New York to England) [22].

Three AUVs were researched for the project: Kongsberg Seaglider, Kongsberg HUGIN, and Liquid Robotics Wave Glider. The table below shows specifications necessary for our system and simulation (speed, duration, and depth rating), which will be discussed later in the report. These AUVs have other capabilities, but these physical specifications are most important to us for the scope of our project.

<b>AUV</b>	<b>Speed</b>	<b>Duration</b>	<b>Depth Rating</b>
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
Liquid Robotics Wave Glider	1.7 m/s	8700 hours	2 meters

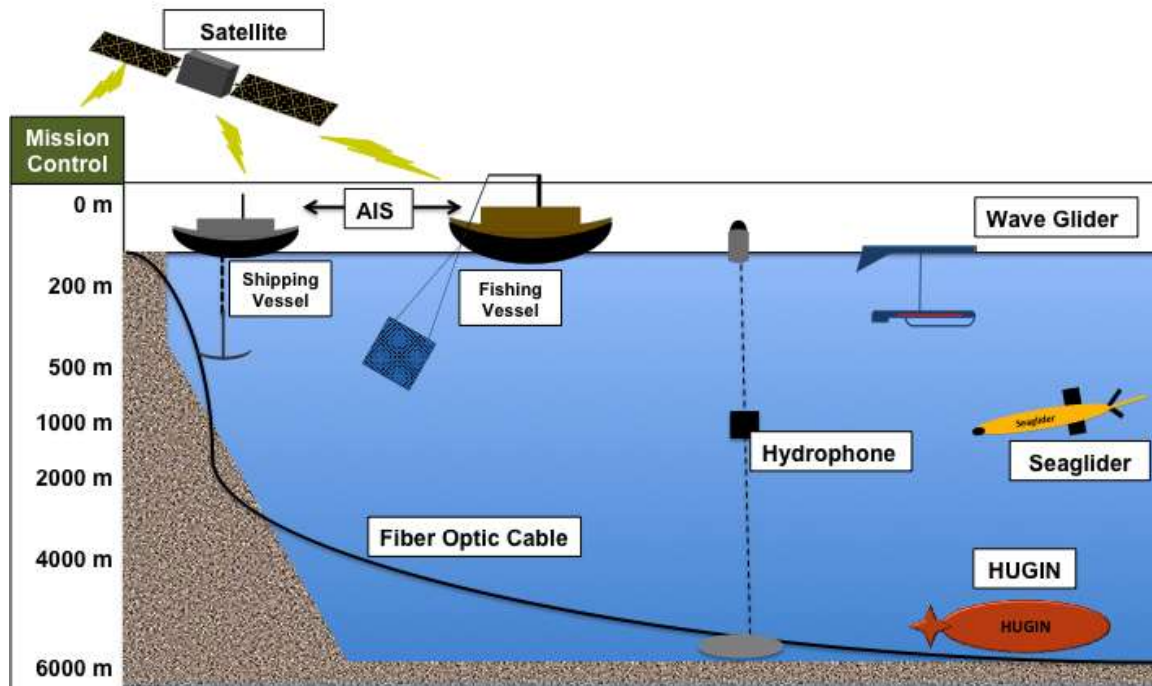
### **6.2.3.3 Hydrophone Array Buoys**

Hydrophone Array Buoys (HB) are groups of stationary nodes positioned along the length of a cable such that they provide coverage of a specified area. In the case of HBs, 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. The effectiveness of this system will depend on the exact range of the hydrophones, number of nodes, and communication with on-shore or ship-based monitors.

There are three components of a hydrophone array buoy: anchor, hydrophone, and surface buoy. The surface buoy floats on the surface of the water and is able to transmit data to Mission Control via satellite. The surface buoy is connected to an array of hydrophones stemming below the surface buoy. These hydrophones are connected to an anchor, maintaining its location. The connections are made with an Ethernet tether. This alternative can be deployed from a ship, allowing for rapid installation [24]. A drawback of HBs is that there must be several hundred installed along the length of the cable. This would increase the maintenance costs and could pose a challenge for maintaining uptime of the system. In the simulation and results section, the high effectiveness of this alternative will be explained in detail.

### **6.3 Alternatives Summary**

The image below provides a summary of all alternatives mentioned in the report thus far. The Design of Experiment will show the way in which the alternatives will be combined to effectively protect the cable.



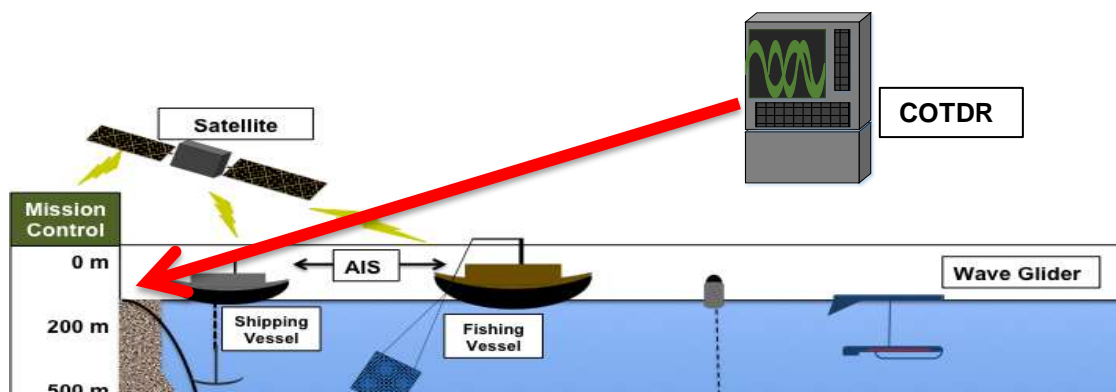
### 6.3 Prevention Alternative

To perform the second function, Prevention and Monitoring, 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 threat identification alternatives (Surface and Underwater) will relay data on threats to Mission Control. The surface threat 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 Hydrophone Array Buoys. 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. It is in the best interest of the ship captain to avoid damaging cables due to the potential harm that the cable could inflict on the vessels equipment.

For intentional threats (sabotage, espionage), prevention will be much more difficult because these actors will be moving quickly and covertly. In the event that we do identify an intentional threat and relay the data to Mission Control, we will send messages to relevant authorities (Governments, USGS, USN) so they can intervene and take necessary action. From there, the authorities will handle the situation and our system will move into the next function, repair organization, if damage has occurred.

#### 6.4 Repair Organization Alternative – Coherent Optical Time Domain Refractometer

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. A method that TCPS will be using to better identify fault location is a Coherent Optical Time Domain Refractometer (COTDR). The COTDR will be located at a Cable Landing Station and operates by sending a pulse of known width down the length of the damaged cable. The light backscatter is measured and it is able to quickly determine the fault location and fault segment as close as 10 meters. COTDRs are not currently equipped at most Cable Landing Stations and can potentially reduce the total repair time of the cable system by a significant amount. The graphic below shows the location at which the COTDR will be placed.





## 7.0 Simulation

### 7.1 Simulation Overview

The goal of our simulation is to determine a solution that provides the best utility for a given infrastructure surveillance case. Three main cases will be simulated: a single design alternative monitoring the entire cable, combinations of design alternatives monitoring the entire cable, and combinations of design alternatives monitoring only the coastal or shallow sections of the cable.

All researched design alternatives have tradeoffs between cost, movement, sensor capabilities, and depth capability that make it unlikely any single alternative will be the best choice by itself. Instead, we want to test hybrid systems of design alternatives with complementary functions. Additionally, the fact that 70% of cable damage occurs in less than 200m of depth indicates that a partial coverage system could potentially have a high utility for a low cost.

Utility will be determined by a combination of factors: ability to detect threats, faults, efficacy of prevention messages, and reduction in number of faults/MTBF and increase in cable availability.

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 pair of 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. Two have been chosen to model, the SEA-US and APX-East cables.

Cable Name	SEA-US	APX-East
Length	15000	12500
CLS #	4	2
Max Depth	5000	6000
Shallow %	41.6	37.6

*Representative cables chosen for simulation*

These cables were chosen since they represent the newest technology coming online in the next several years. The TCPS is being designed with the idea to protect the newest generation of cables, as the new fiber optic technologies available are set to dramatically increase available bandwidth, rendering older cables obsolete within a few years. This can be seen in the bandwidth capacities of these new cables, 20 and 40 Tbps, as opposed to common in-service cable capacities of 0.48, 2.4 and 5.12 Tbps. These new cables represent a huge step up in available bandwidth and cable value.

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. This process is detailed more in section 6.5.

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 (AUVs – HUGIN, SeaGlider, Wave Glider), passive alternatives (Hydrophone bouys), and surface alternatives (AIS).

The simulation is then run for 10 simulated 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 times 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.

## 7.2 Simulation Requirements

**SR 1.0:** The simulation shall model a representative cable system as closely as possible.

**SR 2.0:** The simulation shall generate threats at interarrival times based on research data.

**SR 3.0:** The simulation shall determine the utility of various design alternatives by tracking cost, detection chances, fault prevention and cable downtime reduction.

**SR 4.0:** The simulation shall generate all possible data from random distributions based on collected research.

**SR 5.0:** The simulation shall output results to a comma separated text file that can be analyzed.

**SR 6.0:** The number of simulation replications shall be determined by a 10% halfwidth and 95% confidence interval.

### 7.3 Design of Experiment

Cable	System Type	TCPS Technologies	TCPS Coverage		
			Instant	Per 24 hrs	Total
SEA-US	None	None	0.0%	0.0%	0.0%
SEA-US	AIS Only	4 AIS Recievers	8.0%	8.0%	8.0%
SEA-US	AUV Only	26 HUGIN AUVs	5.5%	36.7%	100.0%
SEA-US	AUV Only	50 SeaGlider AUVs	10.6%	17.9%	100.0%
SEA-US	Hydrophone Only	1000 Hydrophone Bouys	100.0%	100.0%	100.0%
SEA-US	AUV Only	30 Wave Glider AUVs	80.0%	97.8%	100.0%
SEA-US	Hybrid Case 1	4 AIS, 19 HUGIN, 9 SeaGlider	14.0%	38.1%	100.0%
SEA-US	Hybrid Case 2	4 AIS, 1000 Hydrophones	100.0%	100.0%	100.0%
SEA-US	Hybrid Case 3	4 AIS, 81 H. Bouys, 20 HUGINs	29.5%	53.5%	100.0%
SEA-US	Hybrid Case 4	4 AIS, 81 H. Bouys, 12 Wave Gliders	57.3%	64.4%	100.0%
SEA-US	Hybrid Case 5	4 AIS, 231 H. Bouys	32.1%	32.1%	32.1%
SEA-US	Hybrid Case 6	4 AIS, 7 Wave Gliders	14.6%	30.8%	33.3%
SEA-US	Hybrid Case 7	4 AIS, 231 H. Bouys, 7 Wave Gliders	32.1%	32.1%	33.3%
APX-East	None	None	0.0%	0.0%	0.0%
APX-East	AIS Only	2 AIS Recievers	3.2%	3.2%	3.2%
APX-East	AUV Only	21 HUGIN AUVs	6.6%	36.3%	100.0%
APX-East	AUV Only	42 SeaGlider AUVs	12.4%	19.4%	100.0%
APX-East	Hydrophone Only	834 Hydrophone Bouys	100.0%	100.0%	100.0%
APX-East	AUV Only	25 Wave Glider AUVs	80.7%	97.8%	100.0%
APX-East	Hybrid Case 1	2 AIS, 18 HUGIN, 9 SeaGlider	12.1%	38.5%	100.0%
APX-East	Hybrid Case 2	2 AIS, 834 Hydrophones	100.0%	100.0%	100.0%
APX-East	Hybrid Case 3	2 AIS, 234 H. Bouys, 15 HUGINs	68.3%	89.0%	100.0%
APX-East	Hybrid Case 4	2 AIS, 81 H. Bouys, 8 Wave Gliders	49.8%	55.2%	100.0%
APX-East	Hybrid Case 5	2 AIS, 313 H. Bouys	83.3%	83.3%	83.3%
APX-East	Hybrid Case 6	2 AIS, 8 Wave Gliders	29.0%	34.5%	41.6%
APX-East	Hybrid Case 7	2 AIS, 233 H. Bouys, 8 Wave Gliders	41.6%	41.6%	41.6%

The Design of Experiment sets out the specific inputs to the simulation, namely the cable to be simulated and the listing of TCPS technologies monitoring the cable during the simulation.

## 7.4 Simulation Diagram

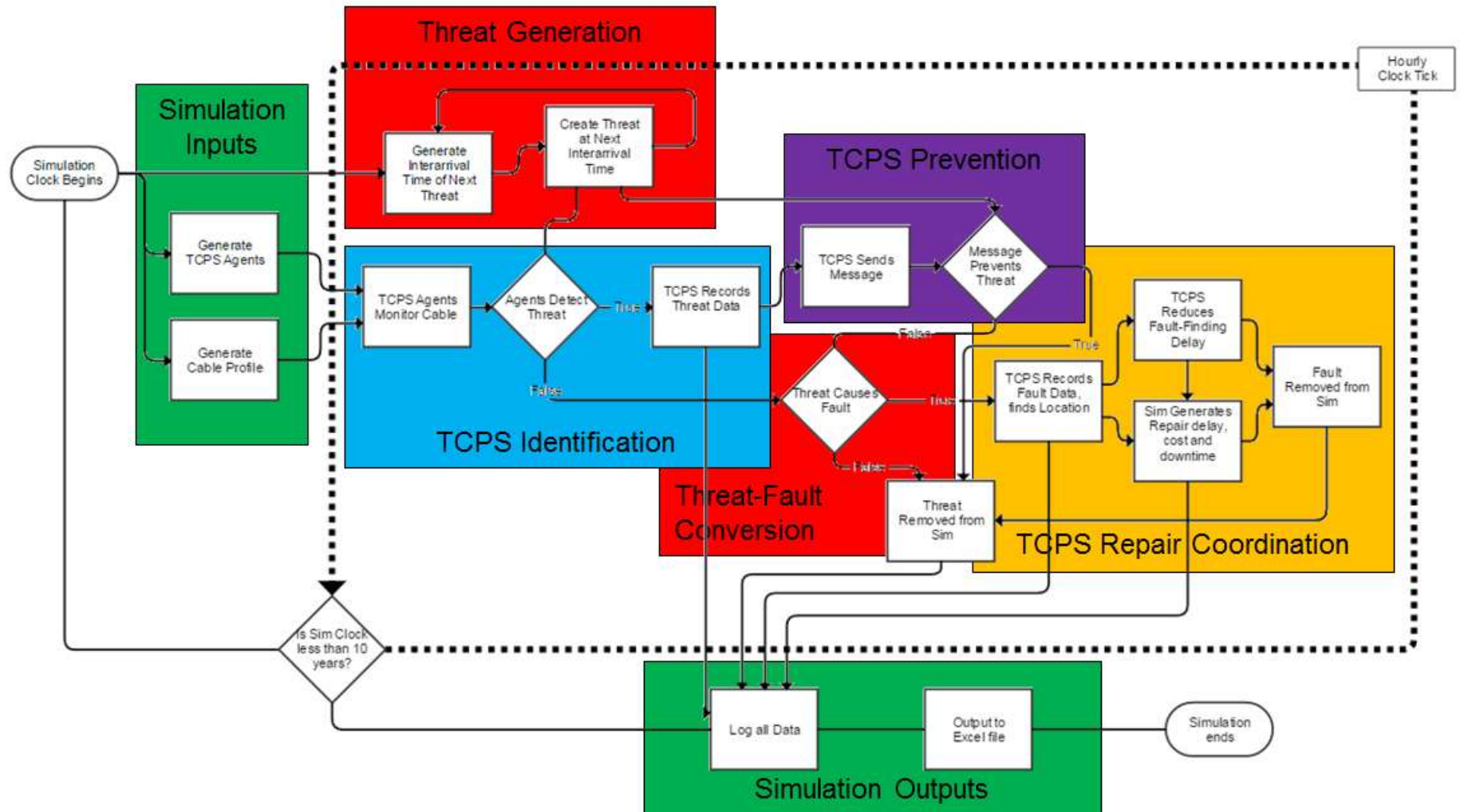


Diagram of main simulation loop and flow of data.

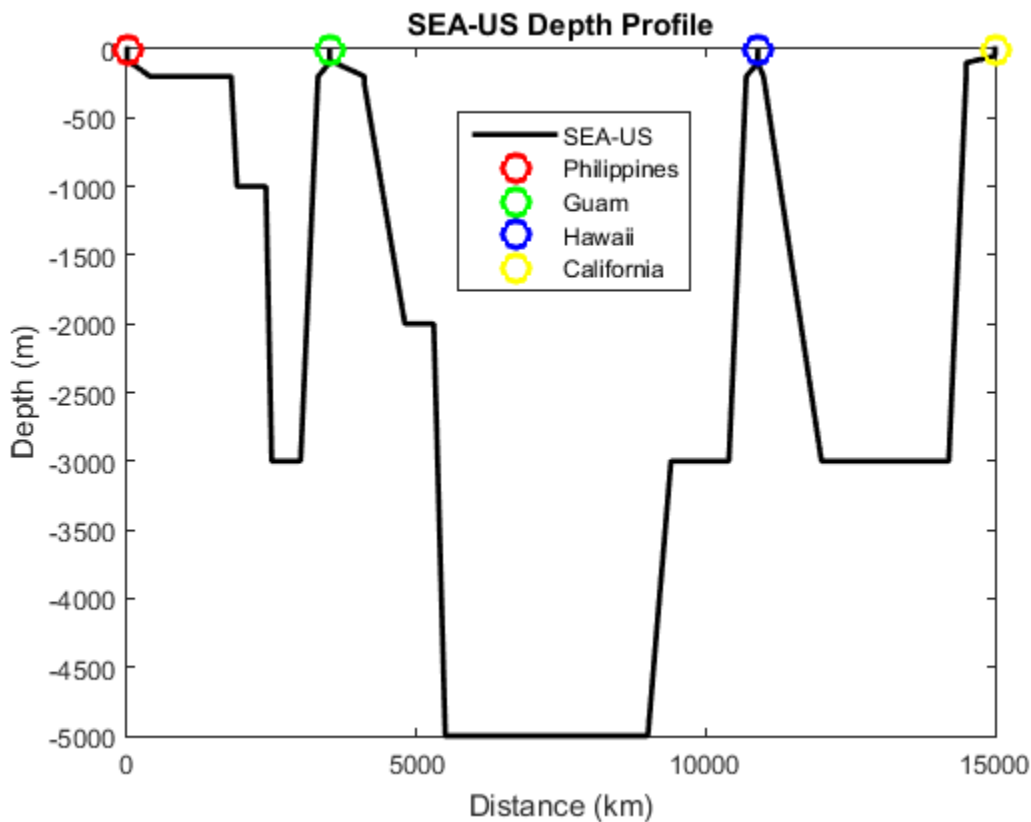
## 7.5 Simulation Parameters

### A. Simulation Inputs

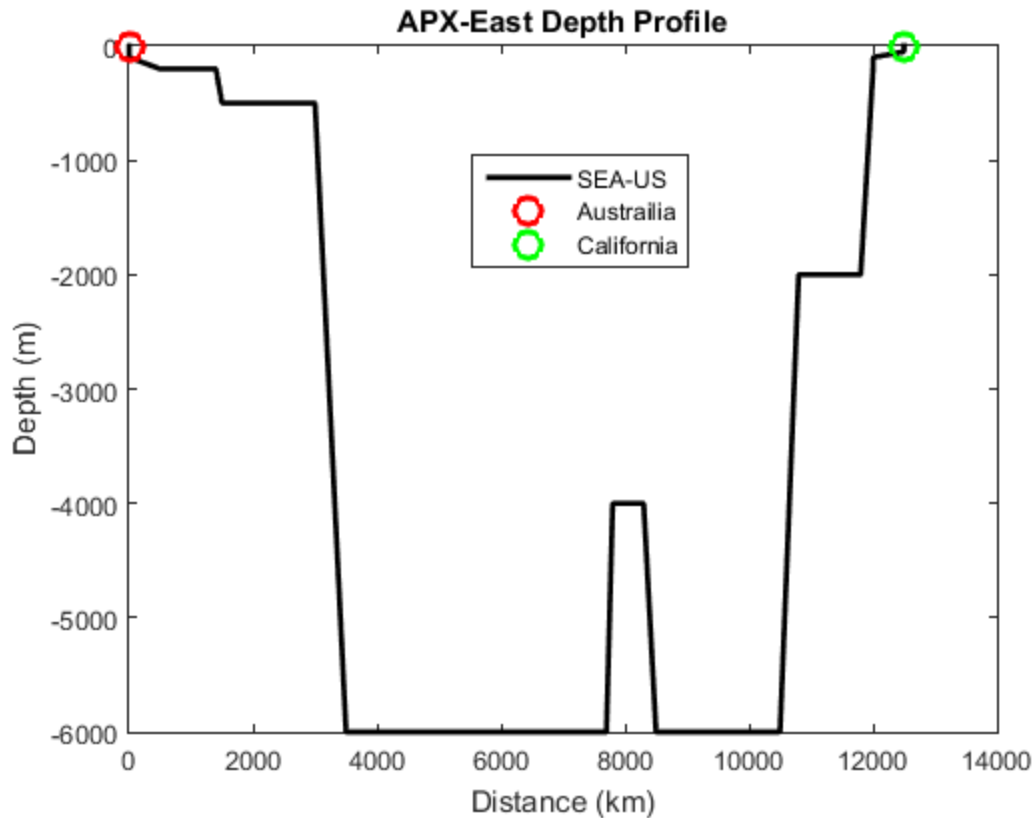
Each simulation has 2 major inputs, the depth profile of the cable to be simulated and the TCPS agent profile, a listing of the monitoring technologies to be deployed.

The cable depth profiles were made by overlaying the cable locations on NOAA bathymetric depth maps. Depth estimates were made along the length of the cable system, which were then programmed into the simulation as a series of equations giving the depth at each kilometer of cable length. Cable landing station (CLS) locations were also programmed into the depth profile, as some design alternatives are shore based.

The simulation uses these depth profiles to model movement of the TCPS agents and to place threats/faults in appropriate locations per fault time, i.e. anchoring threats will only be generated at depths it's possible to such threats to occur.



*Plot of SEA-US cable depth and CLS location profile*



*Plot of APX-East cable depth and CLS location profile*

The second major input to each simulation is the TCPS agent profile. This is a listing of the type, equipped sensors, movement speed/capability, maximum depth and pre-determined ranges for each individual TCPS agent being simulated. For each cable being simulation, 13 agent profiles, or cases, were determined. One case with no agents at all (as-is system), 5 cases with only a single design alternative, 4 cases with 2 or more design alternatives, and 3 cases of 2 or more design alternatives only covering the most likely threat locations for that cable. One sample TCPS agent profile is shown below for one of the hybrid, full coverage cases. Several TCPS profiles have hundreds of agents being simulated, so only one is show as an example.

#	Type	Sensors	Speed	Depth (m)	Range (km)	
1	AIS Receiver	AIS	0	0	0	0
2	Seaglider	Hydrophone	0.9 km/hr	200	0	200
3	Seaglider	Hydrophone	0.9 km/hr	200	150	350
4	Seaglider	Hydrophone	0.9 km/hr	200	300	500
5	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	500	1200
6	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	1200	1900
7	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	1900	2600
8	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	2600	3300
9	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	3300	4000
10	Seaglider	Hydrophone	0.9 km/hr	200	4000	4300
11	AIS Receiver	AIS	0	0	4100	4100
12	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	4000	4700
13	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	4700	5400
14	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	5400	6100
15	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	5000	6100	6800
16	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	5000	6800	7500
17	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	5000	7500	8200
18	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	5000	8200	8900
19	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	5000	8900	9600
20	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	9600	10300
21	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	10300	11000
22	Seaglider	Hydrophone	0.9 km/hr	200	11000	11300
23	Seaglider	Hydrophone	0.9 km/hr	200	11300	11600
24	AIS Receiver	AIS	0	0	11500	11500
25	Seaglider	Hydrophone	0.9 km/hr	200	11600	11800
26	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	11800	12500
27	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	3000	12500	13200
28	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	1000	13200	13800
29	HUGIN	Hydrophone, SAS sonar	7.5 km/hr	200	13800	14500
30	Seaglider	Hydrophone	0.9 km/hr	200	14500	14750
31	Seaglider	Hydrophone	0.9 km/hr	200	14750	15000
32	AIS Receiver	AIS	0	0	15000	15000

*TCPS Agent profile for SEA-US Hybrid Full Coverage Case 1*

*B. Threat Generation and Threat to Fault Conversion*

To generate threats in the simulation, a number of distributions were used. A Poisson distribution to model the threat interarrival times, probability distributions to determine threat type, fault conversion rate, and normal distributions to determine threat loiter time.

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. As there are generally no legal requirements to publish this data, the majority of cable owners keep this information confidential.

Based on the global data of over 300 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
<b>Total</b>	<b>0.821</b>	<b>1</b>	<b>0.5</b>		<b>6.300</b>	<b>1390.4</b>

*Table used to determine threat interarrival rate*

The final interarrival time of 1390.4 hours was then converted to a poisson mean of  $\lambda = 0.000762842$ . Further, a single poisson mean can be used as we're modeling all threats as independent events, so it is mathematically the same to model 6 individual threat type distributions, or one combined distribution.

As threats are generated, a “loiter time” is also generated – this is the time the threat would be endangering the cable. At the end of this time, if the threat is not identified by the end of this loiter time, the simulation checks if the threat has caused a fault with the threat-fault conversion probability. As no data was available to determine these rates, estimated normal distributions were used.

	Threat Probability	Loiter time Distributions [N( $\mu$ , $\sigma$ )]	Threat-Fault conversion probability
Fishing	0.541	N(2, 0.5)	0.05
Anchoring	0.19	N(12, 6)	0.25
Component	0.088	0	1.0
Natural	0.084	N(48, 24)	0.1
Espionage	0.049	N(4380, 1095)	0.0
Sabotage	0.049	N(4, 1)	1.0

*Threat loiter time distributions*

Fishing threats represent a commercial fishing vessel in the area of the cable actively using fishing equipment that may damage the cable system, such as trawl nets. They are only in the cable area for a short time before passing through as they fish. These ships are assumed to have an active AIS transponder on board, as required by law.

When generated, threats exist on the simulated cable until either the loiter time counts down to zero (decremented with the hourly simulation clock), or the TCPS has detected and successfully messaged the threat, removing the it from the simulation.

*C. Threat Types*

Anchoring threats represent large commercial shipping vessels that anchor, or may drop anchor in the cable area. Most anchoring damage is not caused by the initial impact of an anchor, but the movement of a dropped anchor along the seafloor, which tangles the cable.

These fishing and commercial ships are assumed to have an active AIS transponder on board, as required by law. It is also assumed they do not wish to damage the cable system and will leave the immediate cable area when notified of the possible danger.

Component threats represent malfunctions or faults in the hardware of the cable system. There is no way to detect ahead of time or prevent these types of faults, giving them a loiter time of 0 hours and a threat-fault conversion rate of 100%.

Natural threats represent the broad category of faults caused by non-human actors or events. These faults are caused mostly by abrasion of the submarine cable along the seafloor, but can be caused by weather events and large marine animals. These threats cannot be prevented. The threats generated by the simulation are assumed to be of the abrasion (think cable snagged on a rock) or large marine animal type which can be detected by nearby, high-resolution sonar.

Sabotage threats represent intentional hostile human activity against the cable system. These threats cannot be prevented, but time is required to damage the cable system, during which the TCPS agents have a chance to detect the action and alert the authorities (ex. USCG). Sabotage may take the form of scuba divers, small submersibles, and large ships dragging grapnels or equipped with cable-cutting ROVs. Further, illegal fishing activities fall under this category for simulation purposes.

Espionage threats are a special, two part case. First an espionage attempt threat is generated with a loiter time of 6 hours. At the end of the loiter time, an espionage device is attached to the cable. The espionage attempt can be scuba divers, submersibles, or ship-based ROVs and can be detected in the same manner as other threats. However, once the espionage device is attached, it can only be detected by a close range, high-resolution sonar scan. Espionage attempts cannot be prevented, only detected during the attempt. Espionage devices cannot be removed by the TCPS agents, only detected if the agent is very close (< 300m) and equipped with SAS.

It is assumed that any large ship engaged in illegal activity (sabotage, espionage or illegal fishing) will not be broadcasting an AIS signal and cannot be detected or communicated with over the AIS system.

#### D. TCPS Agents

TCPS agents are initialized at the beginning of the simulation as described in the TCPS agent profile for the case to be simulated. They are placed along the cable at the start of their assigned ranges and begin monitoring the cable system as soon as the simulation clock starts. Each agent consists of a platform and one or more sensors. The platforms determine movement speed, maximum depth and which sensors can be installed, while sensors determine detection range and type of threats that can be detected.

Platform	Movement speed (km/hr)	Max Depth (m)	Sensors
Cable Landing Station	0	0	AIS
Tethered Bouy	0	6000	Hydrophone
SeaGlider AUV	0.9	1000	Hydrophone
HUGIN AUV	7.5	6000	SAS, Hydrophone
Wave Glider AUV	3.7	50	AIS, SAS, Hydrophone

*Table of TCPS Agent platforms*

Sensor	Detection radius (km)	Detection area	Threats detected
AIS	200	Surface only	Surface only, Fishing, Anchoring
Hydrophone	16	Surface, Underwater	Fishing, Anchoring, Sabotage, Espionage attempts, but not devices
SAS (Synthetic Aperture Sonar)	0.3	Underwater only	Fishing, Anchoring, Sabotage, Espionage attempts and devices, Natural

*Table of TCPS agent sensor types and capabilities*

Every hourly clock tick of the simulation, all TCPS agents have a chance to detect any threats within their sensors' detection radii, if the threat can be detected by the type of equipped sensor. Agents also travel along the cable at their movement speed on each clock tick.

*E. Fault prevention*

If a threat is detected by a TCPS agent, messages are sent to the threat through either the AIS or VHF radio systems. Only fishing and anchoring faults can be prevented. The TCPS relies on the fact that these faults are accidental, and the threat will leave the area when warned away by the TCPS. For the simulation, this is assigned a simple probability when the threat is sent a message. The probability of success is higher when a threat is detected by AIS, as AIS yields significant data about the threat as well as a communication channel.

Other human activity around the cable system will not respond to messages. Sabotage threats wish to damage the cable system and cannot be prevented. Espionage threats do not wish to damage the cable, but instead want to leave a device on a functioning cable.

Natural and component faults cannot be prevented or communicated with.

*F. Repair and bandwidth loss calculations*

When a fault is simulated, distributions from research data are then used to generate the 3 major delays – notification delay, travel delay, and repair time. The travel delay and repair time are added and multiplied by the hourly repair ship cost (\$12,000/hour) for the total repair cost.

<u>Delay Type</u>	<u>Distribution</u>
Fault finding and Notification	1 + WEIB(6.78, 1.07)
Repair ship travel	1 + WEIB(2.07, 1.26)
Repair time	3 + LOGN(1.73, 2.02)

*Fault repair delay distributions*

These three delay times add together for the total cable downtime. Total downtime is then multiplied by the cable capacity and 10 Gbps monthly rental rate to determine the lost bandwidth cost caused by the fault. This varies on a per cable basis.

	SEA-US	APX-East
10 Gbps rental	\$25,000.00	\$8,500.00
Total Bandwidth Capacity	20 Tbps	40 Tbps
10 Gbps rental units	2000	4000
Monthly Value	\$50,000,000.00	\$34,000,000.00

*Table of bandwidth capacities and costs for simulated cables*

Repair cost is calculated by adding together the repair ship travel and repair times together, then multiplying by an estimated \$12,000 per hour rate. In the real world, cable owners are either members of repair organizations or negotiate individual contracts per repair. Our method of calculating repair cost is instead based on the data for repair cost and time – approximately \$3 million per repair and 1-2 weeks (not including fault finding and notification delays), or \$5952 per hour.

If the fault was detected by the TCPS prior to occurring, a 6 hour reduction in the fault finding and notification delay is removed from the total downtime. This is an area where major improvements can be made, much more than 6 hours. However, we wanted to be very conservative, as improvements would be on a cable by cable basis. Some have good fault-finding capabilities and memberships to repair organizations, while others don't. The former would have minimal delay reductions from the TCPS (6 hrs or less) while the latter could see delay reductions of days or even weeks.

### *G. Replications*

A 10 year clock cycle represents 1 simulation replication for a simulated TCPS design case. Each case is replicated 7700 times to get ensure the statistical significance of our output data. This number was determined by calculating the required replication number to yield a maximum half-width of 10% of the mean with a 95% CI on all our data. The data from a 1000 replication test run was used to generate this data.

## 7.6 Simulation Results

### A. Preliminary Simulation Results

A preliminary simulation was run on the FA-1 cable, a transatlantic cable originally installed in 2001. This simulation was a test that helped to identify ways to iterate the simulation and showed our team the way forward was to focus on installing the TCPS on new generation cables since their value and potential losses from damage at much higher. The results are shown below.

	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*

### B. Sample simulation output

When run, the simulation tracks 27 data points per replication. When the replication is completed, these 27 points are saved to a .csv file that can be read by Excel for analysis. One simulation output file has  $27 \times 7700 = 207900$  individual data points. A sample output page for the SEA-US Hybrid Case 1 simulation is shown on the next few pages:

Replication #	Fishing Threats	Anchoring Threats	Component Threats	Natural Threats	Human Activity Threats	Total Threats	Fishing Threats Detected	Anchoring Threats Detected	Component Threats Detected	Natural Threats Detected	Human Activity Detected	Espionage Devices Detected
0	48	2	2	8	0	60	10	1	0	0	0	0
1	47	2	1	1	3	54	11	2	0	0	0	1
2	56	3	1	10	0	70	17	2	0	0	0	0
3	54	5	1	8	0	68	16	3	0	0	0	0
4	50	6	0	3	1	60	12	0	0	0	0	0
5	55	2	1	5	0	63	15	1	0	3	0	0
6	54	2	0	4	3	63	18	1	0	0	1	1
7	54	10	0	5	1	70	12	3	0	1	0	0
8	50	4	1	4	0	59	17	3	0	1	0	0
9	48	7	1	2	1	59	15	7	0	1	0	0
10	59	6	1	4	2	72	16	3	0	0	0	1
11	53	4	0	1	0	58	18	1	0	0	0	0
12	60	6	0	2	0	68	17	3	0	0	0	0
13	62	3	0	5	1	71	19	2	0	2	0	0
14	50	2	1	6	5	64	16	1	0	1	0	1
15	49	4	1	5	0	59	17	1	0	0	0	0
16	41	6	0	10	0	57	14	2	0	1	0	0
17	70	5	1	6	0	82	23	3	0	2	0	0
18	54	5	0	7	0	66	19	1	0	0	0	0
19	53	7	0	2	1	63	20	3	0	0	0	1
20	57	7	1	2	1	68	18	3	0	0	0	0
21	56	2	0	2	0	60	19	1	0	0	0	0
22	59	6	0	4	0	69	18	1	0	0	0	0
23	44	7	1	7	1	60	13	3	0	0	0	0
24	56	1	0	4	2	63	22	1	0	1	0	0
25	56	2	2	6	1	67	14	0	0	1	0	0
26	39	3	2	4	1	49	15	1	0	1	0	0
27	43	7	0	4	1	55	15	3	0	0	0	0
28	47	3	0	1	1	52	15	2	0	0	0	0
29	62	2	0	8	0	72	16	0	0	2	0	0
30	50	7	0	5	2	64	17	3	0	0	1	0

Fishing Faults	Anchoring Faults	Component Faults	Natural Faults	Sabotage Faults	Espionage Devices	Threats Detected	Total Faults	Faults Prevented	Faults Detected Not Prevented	Total Downtime	Total Repair Cost	Total Lost Bandwidth Cost	MTBF
0	1	2	0	0	0	11	3	0	1	830	6707945	56586027	29200
1	0	1	0	2	1	14	4	1	0	1187	9715239	80886346	21900
4	3	1	1	0	0	19	9	0	2	2926	24127197	199349247	9733
2	0	1	1	0	0	19	4	1	0	1129	8813827	76934362	21900
1	1	0	0	1	0	12	3	0	0	861	6913012	58627577	29200
3	0	1	1	0	0	19	5	1	0	1443	11517402	98239011	17520
2	0	0	0	2	1	21	4	2	1	995	8112493	67750768	21900
2	1	0	1	1	0	16	5	1	0	1419	10750356	96640218	17520
2	0	1	1	0	0	21	4	0	1	1522	13360687	103584235	21900
1	0	1	0	1	0	23	3	1	0	1006	8849381	68490208	29200
2	2	1	0	0	2	20	5	0	0	1425	11108519	97090225	17520
0	0	0	0	0	0	19	0	1	0	0	0	0	0
4	1	0	0	0	0	20	5	3	2	1162	8360584	79159550	17520
1	0	0	0	0	1	23	1	2	0	247	1901984	16851909	87600
0	0	1	1	3	2	19	5	0	0	1463	12026349	99644212	17520
2	0	1	0	0	0	18	3	2	0	1055	8934115	71801197	29200
0	1	0	1	0	0	17	2	0	0	514	3858227	35018375	43800
2	1	1	0	0	0	28	4	1	1	1126	9069765	76774973	21900
1	0	0	3	0	0	20	4	0	0	1349	11040032	91874338	21900
2	1	0	1	0	1	24	4	0	1	1029	7540799	70194987	21900
3	0	1	0	0	1	21	4	1	0	992	7318472	67606264	21900
0	0	0	0	0	0	20	0	0	0	0	0	0	0
4	0	0	0	0	0	19	4	0	1	1354	11801289	92215945	21900
1	1	1	0	1	0	16	4	0	1	1302	11058380	88671585	21900
0	0	0	0	1	1	24	1	0	0	336	3216688	22899370	87600
0	0	2	1	0	1	15	3	1	0	823	6136025	56038809	29200
2	0	2	1	1	0	17	6	2	1	1967	16405274	134080582	14600
4	0	0	0	1	0	18	5	1	0	1548	12613735	105444047	17520
0	0	0	0	0	1	17	0	0	0	0	0	0	0
2	2	0	1	0	0	18	5	0	0	1703	14674792	116018657	17520
1	1	0	1	2	0	21	5	1	1	1802	15301347	122726278	17520

### C. SEA-US Simulation output analysis

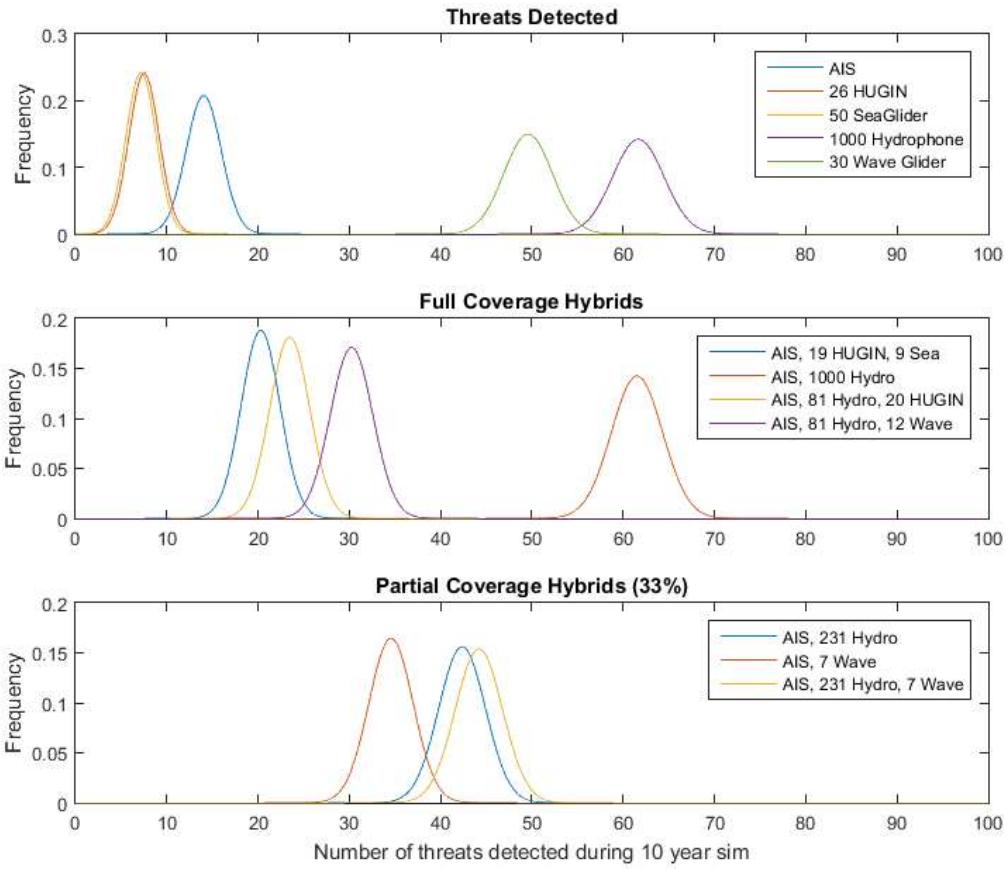
We analyzed the simulation focusing on three major areas: ability to detect threats, ability to prevent faults, and effect on system costs. First, threats detected on the SEA-US cable:

<b>Threats</b>			
	Total	Detected	%
As-Is	66.6	0.0	0%
AIS	66.7	14.0	21%
HUGIN	66.8	7.5	11%
SeaGlider	66.8	7.2	11%
<b>Hydrophone</b>	<b>66.8</b>	<b>61.7</b>	<b>92%</b>
Wave Glider	66.8	49.6	74%
Hybrid Case 1	66.8	20.3	30%
<b>Hybrid Case 2</b>	<b>66.7</b>	<b>61.5</b>	<b>92%</b>
Hybrid Case 3	66.8	23.5	35%
Hybrid Case 4	66.9	30.2	45%
Hybrid Case 5	66.8	42.4	63%
Hybrid Case 6	66.9	34.6	52%
<b>Hybrid Case 7</b>	<b>66.8</b>	<b>44.2</b>	<b>66%</b>

*Table of threats detected by TCPS agent cases*

The bolded cases of Hydrophone, Hybrid Case 2 and Hybrid case 7 are the highest performing cases in this simulation. Hydrophone and Hybrid Case 2 clearly have the best threat detection rates, with 92% of all system threats being detected. Hybrid Case 7 has only 66%, but it is a partial coverage case with significantly lower cost and cable coverage, so its performance is impressive.

A plot of the threat detection distributions for each case is below. As the distribution peaks move further to the right, the more threats were detected.



*Plots of SEA-US simulation threat detection*

Next, fault prevention.

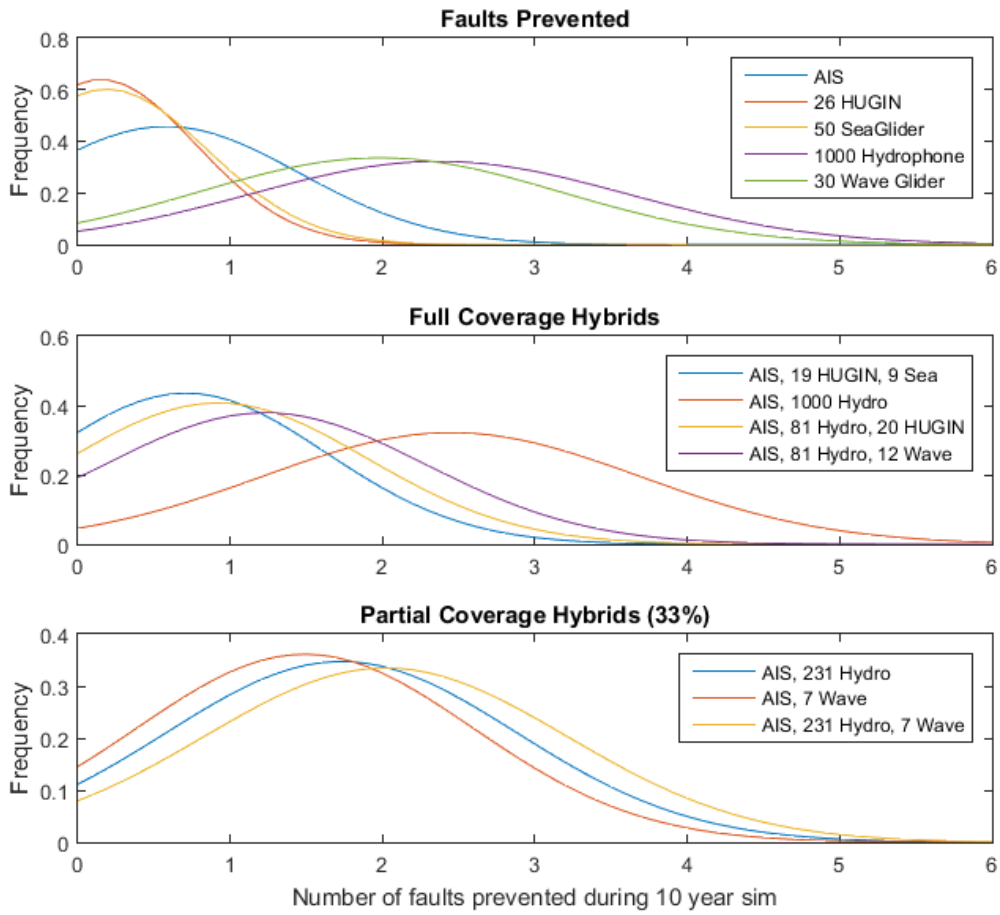
### Faults

	Total	Prevented	%	Detected	%
<b>As-Is</b>	4.4	0.00	0%	0.00	0%
AIS	3.8	0.58	13%	0.14	3%
HUGIN	4.2	0.15	4%	0.25	6%
SeaGlider	4.2	0.19	4%	0.21	5%
<b>Hydrophone</b>	<b>2.1</b>	<b>2.37</b>	<b>53%</b>	<b>1.21</b>	<b>27%</b>
Wave Glider	2.5	1.98	45%	0.52	12%
Hybrid Case 1	3.7	0.71	16%	0.36	8%
<b>Hybrid Case 2</b>	<b>1.9</b>	<b>2.45</b>	<b>56%</b>	<b>1.05</b>	<b>24%</b>
Hybrid Case 3	3.5	0.92	21%	0.43	10%
Hybrid Case 4	3.2	1.23	28%	0.38	9%
Hybrid Case 5	2.7	1.73	39%	0.77	18%
Hybrid Case 6	3.0	1.49	34%	0.34	8%
<b>Hybrid Case 7</b>	<b>2.4</b>	<b>2.02</b>	<b>45%</b>	<b>0.62</b>	<b>14%</b>

*Table of faults prevented or detected by TCPS agent cases*

Again, the Hydrophone, Hybrid 2 and 7 cases are the best performers. Both Hydrophone and Hybrid 2 are able to prevent over 50% of faults and detect over 20% of occurring faults. Partial coverage Hybrid 7 is able to prevent 45% and detect 14% of occurring faults, the best of the partial coverage cases. Detecting a fault is beneficial if unable to prevent the fault.

Below is a plot of the fault prevention. Distribution peaks further to the right are cases that prevented more faults.



*Plots of SEA-US simulation threat detection*

Next is the effect of each TCPS case on the costs to the cable system.

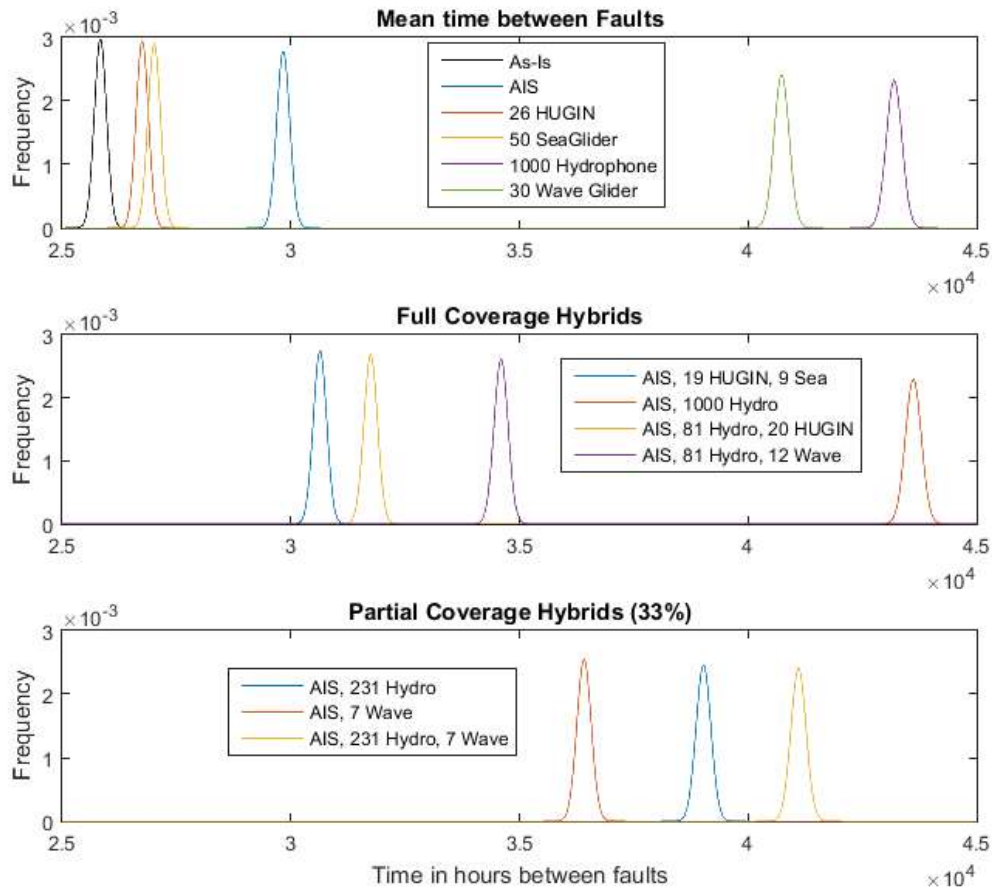
### Costs

	Downtime	Repair	Bandwidth	MTBF (hrs)	Availability
As-Is	1330	\$10,700,000	\$90,300,000	25800	98.48%
AIS	1150	\$9,300,000	\$78,500,000	29800	98.69%
HUGIN	1270	\$10,300,000	\$86,500,000	26800	98.55%
SeaGlider	1260	\$10,200,000	\$86,200,000	27000	98.56%
<b>Hydrophone</b>	<b>620</b>	<b>\$5,000,000</b>	<b>\$42,200,000</b>	<b>43200</b>	<b>99.29%</b>
Wave Glider	740	\$6,000,000	\$50,200,000	40700	99.16%
Hybrid Case 1	1100	\$8,900,000	\$75,100,000	30600	98.74%
<b>Hybrid Case 2</b>	<b>580</b>	<b>\$4,700,000</b>	<b>\$39,300,000</b>	<b>43600</b>	<b>99.34%</b>
Hybrid Case 3	1060	\$8,500,000	\$72,000,000	31700	98.79%
Hybrid Case 4	950	\$7,700,000	\$65,000,000	34600	98.92%
Hybrid Case 5	790	\$6,400,000	\$54,000,000	39000	99.10%
Hybrid Case 6	890	\$7,200,000	\$60,400,000	36400	98.98%
<b>Hybrid Case 7</b>	<b>730</b>	<b>\$5,900,000</b>	<b>\$49,600,000</b>	<b>41100</b>	<b>99.17%</b>

*Table of costs (\$ and downtime) for each case*

For the As-Is case, the simulated cable had over \$10 million in repair costs and over \$90 million in bandwidth losses. It also experienced 1330 hours of downtime, or 55 days of cable downtime. The cable availability was only 98.48%, which is very low for network applications. The Hydrophone, Hybrid 2 and Hybrid 7 cases were again the best performing cases for this simulation. The Hybrid 2 case reduced the approximate repair costs by \$6 million, and reduced bandwidth losses by \$51 million. Mean time between failures increased from 25800 hours to 43600 hours, or from a failure every 2.94 years, to every 4.97 years, over a 2 year mean increase in time between faults. Cable availability similarity increased to 99.34%, an increase of 0.86 percentage points. The Hydrophone and Hybrid 7 cases created similar reductions in costs and downtime.

Below is a plot of the MTBF for these cases. Distribution peaks further to the right are cases that most increased the MTBF.



*Plots of SEA-US MTBF changes*

Overall the Hydrophone, Hybrid 2 and 7 cases had the best results. All three cases are either fully based on Hydrophones, or Hydrophones make up the bulk of the TCPS agents. Hydrophones are immobile and can't use all the sensor types, or detect all threats, but their ability to be permanently deployed along the entire cable and constantly monitoring makes them the best performing alternative.

The HUGIN and SeaGlider AUVs were the worst performing. Their relatively short ranges and slow move speeds meant they simply couldn't cover enough of the cable length to detect most threats before the threats either caused a fault or were removed. HUGINs in particular have excellent sensors and can detect nearly all threats, but their inability to monitor large sections of the cable at once rendered them less capable in this application.

All the sensors researched are more than capable of detecting threats in their detection range. The biggest problem for this project is developing a system that can monitor very large areas of the ocean.

*D. APX-East Simulation results*

For our second simulation, we ran similar TCPS agent cases on the APX-East cable system. The cases are very similar, except the partial coverage hybrids were modified to better suit this cable. Refer to the Design of Experiment in section 6.3 for the changes.

Results were analyzed for threat detection, fault prevention and cost reduction.

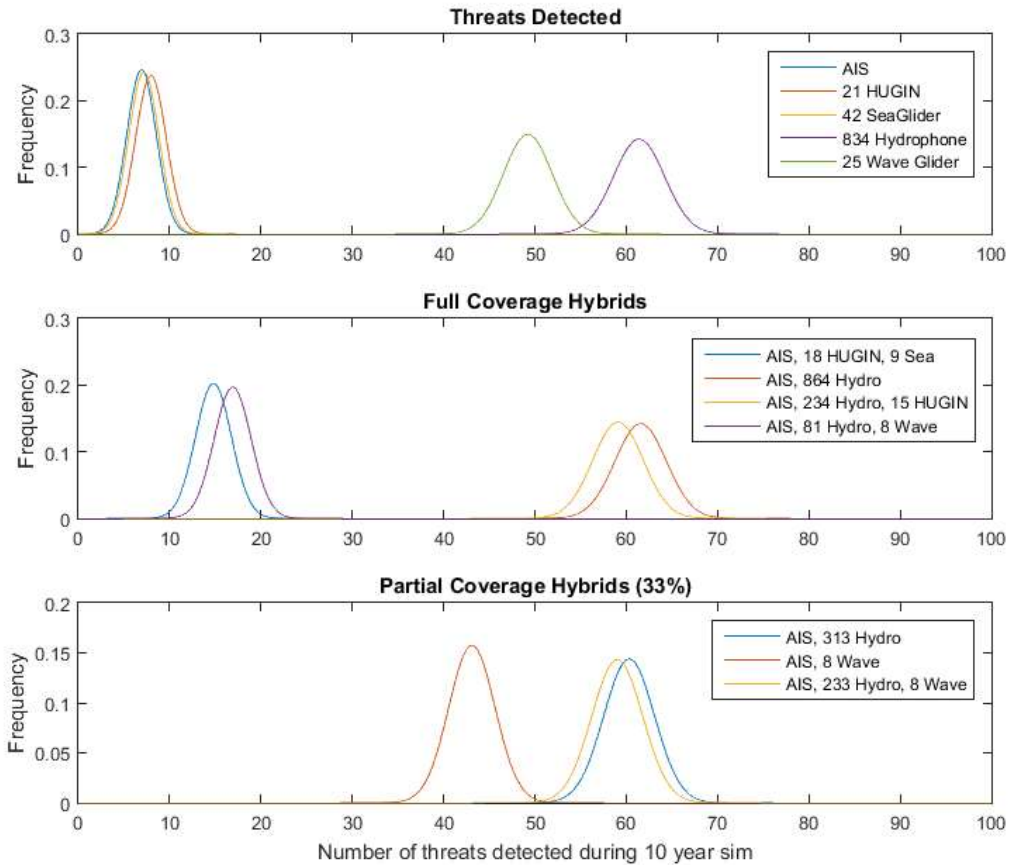
<b>Threats</b>			
	Total	Detected	%
<b>As-Is</b>	66.6	0.0	0%
AIS	66.6	6.9	10%
HUGIN	66.9	8.0	12%
SeaGlider	66.8	7.2	11%
<b>Hydrophone</b>	<b>66.6</b>	<b>61.4</b>	<b>92%</b>
Wave Glider	66.9	49.2	74%
Hybrid Case 1	66.9	14.9	22%
<b>Hybrid Case 2</b>	<b>66.8</b>	<b>61.6</b>	<b>92%</b>
<b>Hybrid Case 3</b>	<b>66.7</b>	<b>59.1</b>	<b>89%</b>
Hybrid Case 4	66.9	16.9	25%
<b>Hybrid Case 5</b>	<b>66.8</b>	<b>60.3</b>	<b>90%</b>
Hybrid Case 6	66.7	43.1	65%
<b>Hybrid Case 7</b>	<b>66.7</b>	<b>59.0</b>	<b>89%</b>

*Table of threat detection rates for APX-East simulation cases*

For the APX simulation, several cases scored very well on threat detection. This increase in performance is attributable to two reasons: the simpler profile of the APX cable, and better planning of the hybrid cases.

The APX cable has only two cable landing stations, and most of its length is deep underwater, making it safer from many threats. Therefore a relatively smaller area of the cable needs to be protected. This difference made the partial coverage cases much more effective in detecting threats, as more threats were present in the small area monitored. This difference can also be seen in the decrease of performance in the AIS case, as there are only two CLS, there can only be two AIS nodes, cutting the coverage area in half against the amount covered by AIS for the SEA-US cable.

Our team designed the hybrid cases for this cable after analyzing the results from the SEA-US sim. This led to the increase in performance see here. Further data, especially the confidential, real world data held by cable owners could be further used to refine the TCPS agent design cases.



*Plots of threat detection for the APX sim*

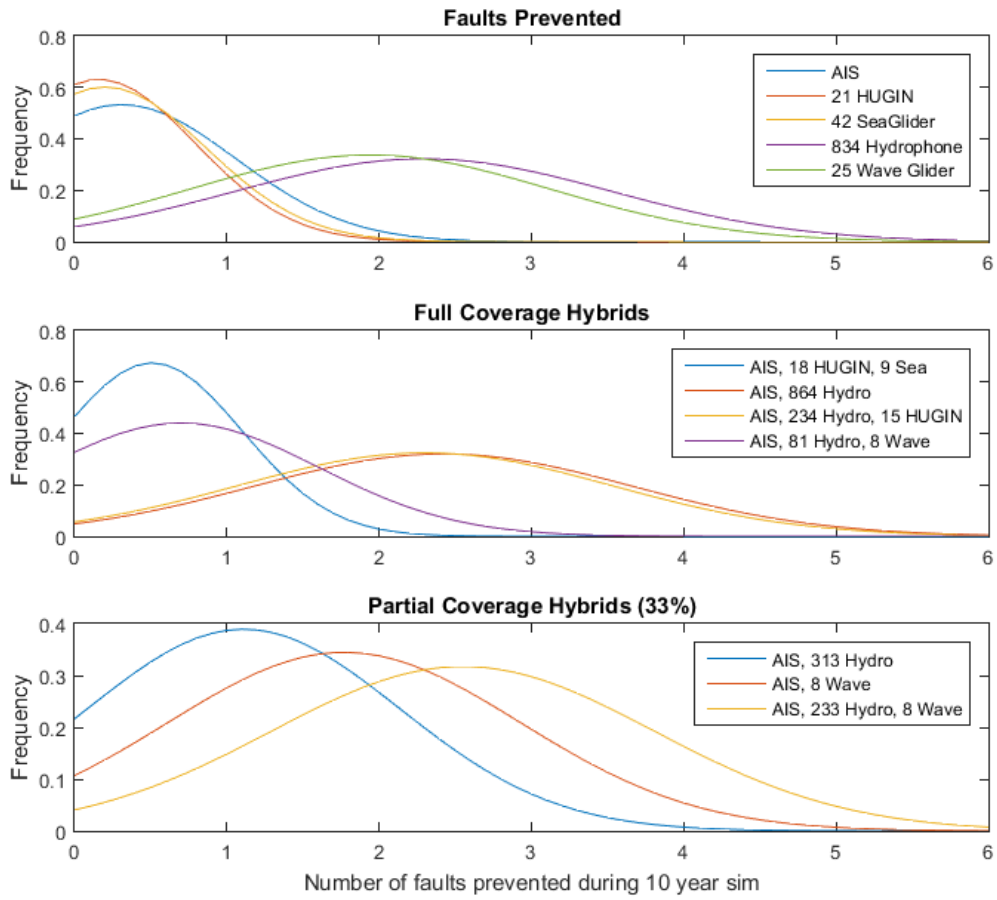
This increase in performance is also evident on the plots above. The Hydrophone and Hybrid 2 (Hydrophone + AIS) cases are again the highest performers, but two of the partial coverage cases and another full coverage hybrid case are also scoring high on threat detection.

### Faults

	Total	Prevented	%	Detected	%
<b>As-Is</b>	4.4	0.00	0%	0.00	0%
AIS	4.1	0.31	7%	0.14	3%
HUGIN	4.3	0.16	4%	0.27	6%
SeaGlider	4.2	0.20	5%	0.20	5%
<b>Hydrophone</b>	<b>2.1</b>	<b>2.29</b>	<b>53%</b>	<b>1.17</b>	<b>27%</b>
Wave Glider	2.4	1.94	44%	0.51	12%
Hybrid Case 1	3.9	0.52	12%	0.35	8%
<b>Hybrid Case 2</b>	<b>1.9</b>	<b>1.98</b>	<b>51%</b>	<b>1.10</b>	<b>28%</b>
<b>Hybrid Case 3</b>	<b>2.1</b>	<b>2.30</b>	<b>52%</b>	<b>1.12</b>	<b>25%</b>
Hybrid Case 4	3.7	0.70	16%	0.24	6%
<b>Hybrid Case 5</b>	<b>2.1</b>	<b>2.38</b>	<b>54%</b>	<b>1.11</b>	<b>25%</b>
Hybrid Case 6	2.6	1.77	40%	0.42	10%
<b>Hybrid Case 7</b>	<b>1.8</b>	<b>2.55</b>	<b>58%</b>	<b>0.85</b>	<b>19%</b>

*Table of fault prevent data for the APX sim*

Again, there are 5 strong cases for fault prevention and detection. The Hybrid Case 7 has the highest prevention at 58%, but 4 others are also over 50% fault prevention. This cable in particular is a good candidate for a partial coverage case due its low number of CLSs and high average depth.



*Plot of faults prevented*

The plot above shows the same fault prevention results. Five cases with good results.

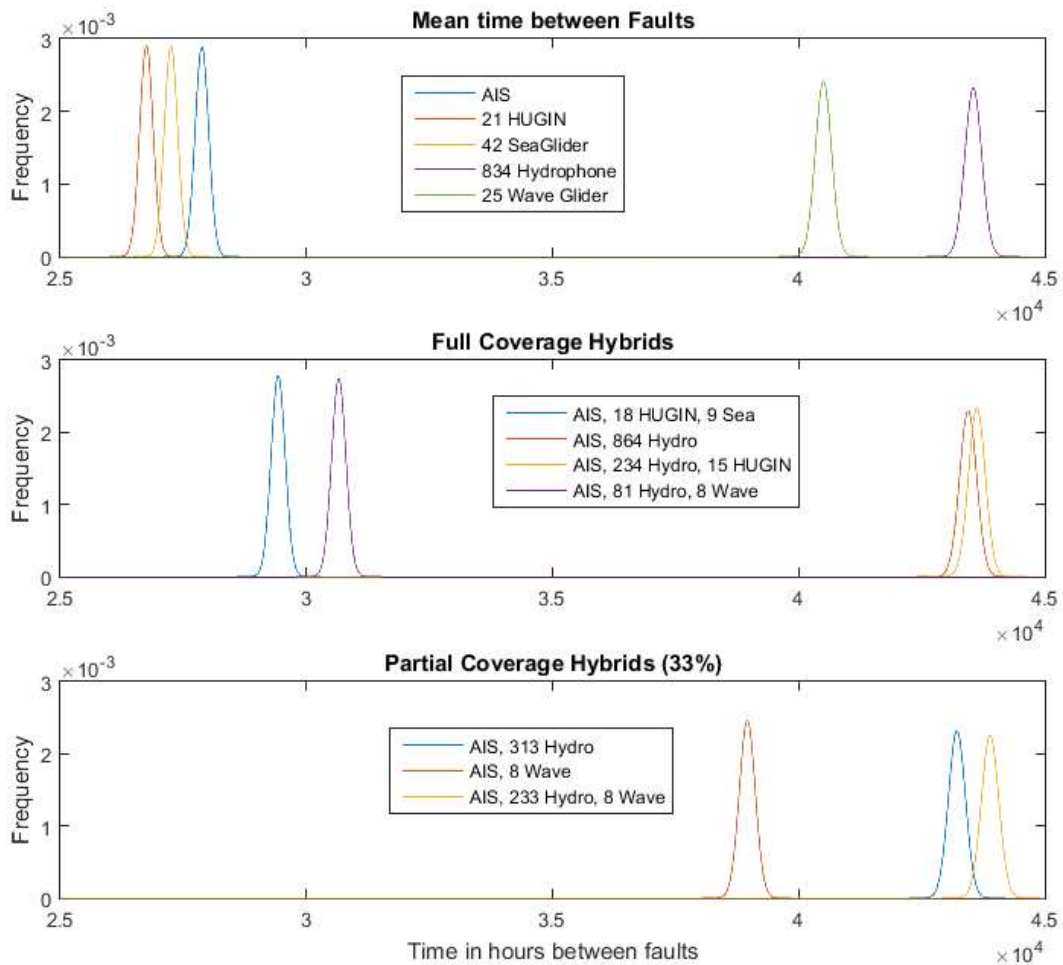
### Costs

	Downtime	Repair	Bandwidth	MTBF (hrs)	Availability
<b>As-Is</b>	1330	\$10,700,000	\$58,600,000	25600	98.48%
AIS	1230	\$9,900,000	\$54,100,000	27900	98.60%
HUGIN	1290	\$10,400,000	\$56,700,000	26700	98.53%
SeaGlider	1250	\$10,100,000	\$55,200,000	27200	98.57%
<b>Hydrophone</b>	<b>610</b>	<b>\$5,000,000</b>	<b>\$26,900,000</b>	<b>43500</b>	<b>99.30%</b>
Wave Glider	730	\$5,900,000	\$32,200,000	40500	99.17%
Hybrid Case 1	1160	\$9,400,000	\$51,300,000	29400	98.68%
<b>Hybrid Case 2</b>	<b>590</b>	<b>\$4,800,000</b>	<b>\$26,000,000</b>	<b>43400</b>	<b>99.33%</b>
<b>Hybrid Case 3</b>	<b>630</b>	<b>\$5,100,000</b>	<b>\$27,800,000</b>	<b>43600</b>	<b>99.28%</b>
Hybrid Case 4	1110	\$8,900,000	\$48,700,000	30700	98.73%
<b>Hybrid Case 5</b>	<b>610</b>	<b>\$5,000,000</b>	<b>\$27,100,000</b>	<b>43200</b>	<b>99.30%</b>
Hybrid Case 6	790	\$6,400,000	\$53,700,000	39000	99.10%
<b>Hybrid Case 7</b>	<b>550</b>	<b>\$4,500,000</b>	<b>\$24,300,000</b>	<b>43900</b>	<b>99.37%</b>

*Table of costs for the APX sim cases*

For the As-Is case, the APX sim showed very similar results to the SEA sim. Over \$10 million in repair costs, 1330 hours of downtime, MTBF is just under 3 years (2.92 years) and availability in the mid-98%. The major difference is in the bandwidth losses. The overall value is lower for the APX cable, due to the lower 10 Gbps monthly rental rate (\$8,500 vs. \$25,000).

The five bolded cables all save millions in repair costs and lost bandwidth, but the Hybrid 7 case is the best, saving \$6.2 million on repairs, \$34.3 million on lost bandwidth costs, increasing the MTBF by 18300 hours (2.09 years) and increasing availability by 0.89 percentage points.



*Plot of MTBF increases for the APX sim cases*

It's clear from all the above results that case with high numbers of hydrophone buoys are the most effective at identifying threats, preventing faults, and reducing costs/downtime to the cable system.

## 7.7 Sensitivity Analysis

### *A. Motivation for sensitivity analysis*

Due to the lack of some data, assumptions had to be made to develop the simulation. Two of the largest assumptions were the detection probability for the sensors and the efficacy of the messages to prevent faults. We performed sensitivity analysis on these probabilities in order to determine if the TCPS would still be effective if the sensors and prevention messages had lower probabilities of success.

For the sensors, there is ample data to show they can all detect threats we are concerned about, given enough time and proximity to the threat. Software also currently exists that can automatically analyze data from the sensors in order to detect threats. For example, hydrophones have been in use since the 60s, and one of their primary uses was long-range detection of submarines. The commercial vessels we are concerned about are most likely easier to detect than submarines, but there is still some uncertainty.

AIS is a similarly robust technology and is currently used to globally track commercial ships. The limitation of the technology is the need to be in range of an AIS receiver, or for the ship to have satellite communications, neither of which is a guarantee. This lends uncertainty to the ability of AIS to detect threats.

SAS is the most cutting edge sonar technology in wide use and it can take high-resolution sonar images of many potential threats. However, it does require either software or human analysis on the images to detect threats, which introduces uncertainty.

### *B. Sensitivity on sensor detection*

For the first simulation, the probability of a sensor detecting a threat in its detection radius was 0.95. For the sensitivity analysis, we've reduced that to 0.75 and re-run all cases of the SEA-US simulation.

Below are the results for the SEA-US sim at reduced detection probabilities.

### Threats Detected

	95% Detection		75% Detection		Difference	
	Detected	%	Detected	%	Detected	%
As-Is	0.0	0%	0.0	0%	0.0	0%
AIS	14.0	21%	13.4	20%	-0.6	96%
HUGIN	7.5	11%	6.9	10%	-0.6	92%
SeaGlider	7.2	11%	6.8	10%	-0.4	95%
Hydrophone	61.7	92%	61.1	91%	-0.5	99%
Wave Glider	49.6	74%	47.2	71%	-2.3	95%
Hybrid Case 1	20.3	30%	19.1	29%	-1.2	94%
<b>Hybrid Case 2</b>	<b>61.5</b>	<b>92%</b>	<b>61.3</b>	<b>92%</b>	<b>-0.2</b>	<b>100%</b>
Hybrid Case 3	23.5	35%	22.9	34%	-0.6	97%
Hybrid Case 4	30.2	45%	29.4	44%	-0.8	97%
Hybrid Case 5	42.4	63%	41.9	63%	-0.5	99%
Hybrid Case 6	34.6	52%	33.2	50%	-1.3	96%
<b>Hybrid Case 7</b>	<b>44.2</b>	<b>66%</b>	<b>44.1</b>	<b>66%</b>	<b>-0.1</b>	<b>100%</b>

*Table of threats detected by TCPS agents with 95% and 75% sensor detection probabilities*

At a 20 percentage point reduction in sensor detection, the number and % of threats detected by the TCPS cases remained remarkably similar. The cases most affected by the reduction in sensor detection chance were the Wave Glider, Hybrid Case 1 and Hybrid Case 6. The least affected cases were Hybrid Case 2 and 7. These cases were likely the least affected since they have significant overlap in detection radii in the coverage areas. The more affected cases depended more on Wave Gliders or other AUVs without much sensor overlap in monitored areas.

### Faults Prevented

	95% Detection		75% Detection		Difference	
	Prevented	%	Prevented	%	Prevented	%
<b>As-Is</b>	0.00	0%	0.00	0%	0.0	0%
AIS	0.58	13%	0.46	11%	-0.1	80%
HUGIN	0.15	4%	0.12	3%	0.0	79%
SeaGlider	0.19	4%	0.14	3%	0.0	76%
Hydrophone	2.37	53%	1.96	44%	-0.4	83%
Wave Glider	1.98	45%	1.61	36%	-0.4	81%
Hybrid Case 1	0.71	16%	0.58	13%	-0.1	82%
Hybrid Case 2	2.45	56%	2.08	47%	-0.4	85%
Hybrid Case 3	0.92	21%	0.75	17%	-0.2	82%
<b>Hybrid Case 4</b>	<b>1.23</b>	<b>28%</b>	<b>1.07</b>	<b>24%</b>	<b>-0.2</b>	<b>87%</b>
Hybrid Case 5	1.73	39%	1.46	33%	-0.3	85%
Hybrid Case 6	1.49	34%	1.24	28%	-0.3	83%
<b>Hybrid Case 7</b>	<b>2.02</b>	<b>45%</b>	<b>1.76</b>	<b>40%</b>	<b>-0.3</b>	<b>87%</b>

*Table of faults prevented by TCPS agents with 95% and 75% sensor detection probabilities*

For faults prevented, we see a significant effect from the reduction of sensor detection probability. Prevention is reduced to 76% of the original value for the SeaGlider case in the worst case, and 87% of its original value for Hybrid cases 4 and 7. Again, significant overlap in coverage is the likely reason these cases are less affected by the reduced detection probability.

	95% Detection		75% Detection		Difference			
	Downtime	Total Costs	Downtime	Total Costs	Downtime	%	Total Costs	%
<b>As-Is</b>	1330	\$101,000,000	1320	\$100,800,000	-10.0	99%	-\$200,000	100%
AIS	1150	\$87,800,000	1180	\$89,900,000	30.0	103%	\$2,100,000	102%
HUGIN	1270	\$96,800,000	1290	\$98,400,000	20.0	102%	\$1,600,000	102%
SeaGlider	1260	\$96,400,000	1290	\$98,100,000	30.0	102%	\$1,700,000	102%
Hydrophone	620	\$47,200,000	740	\$56,300,000	120.0	119%	\$9,100,000	119%
Wave Glider	740	\$56,200,000	840	\$64,100,000	100.0	114%	\$7,900,000	114%
Hybrid Case 1	1100	\$84,000,000	1140	\$87,100,000	40.0	104%	\$3,100,000	104%
Hybrid Case 2	580	\$44,000,000	690	\$52,800,000	110.0	119%	\$8,800,000	120%
Hybrid Case 3	1060	\$80,500,000	1090	\$82,900,000	30.0	103%	\$2,400,000	103%
Hybrid Case 4	950	\$72,700,000	1010	\$77,100,000	60.0	106%	\$4,400,000	106%
Hybrid Case 5	790	\$60,400,000	870	\$66,400,000	80.0	110%	\$6,000,000	110%
Hybrid Case 6	890	\$67,600,000	950	\$72,600,000	60.0	107%	\$5,000,000	107%
Hybrid Case 7	730	\$55,500,000	800	\$61,000,000	70.0	110%	\$5,500,000	110%

*Table of cost changes by TCPS agents with 95% and 75% sensor detection probabilities*

The increases in downtime due to the reduced detection chance ranged from +2% for the HUGIN and SeaGlider cases to +19% for the Hydrophone and Hybrid 2 cases. Total costs increased similarly, with increases between 2% and 20% for different cases.

**Change due to decrease in detection probability**

	Threats	Faults	Downtime	Costs	Average
AIS	96%	80%	103%	102%	<b>7%</b>
HUGIN	92%	79%	102%	102%	<b>8%</b>
SeaGlider	95%	76%	102%	102%	<b>8%</b>
Hydrophone	99%	83%	119%	119%	<b>14%</b>
Wave Glider	95%	81%	114%	114%	<b>13%</b>
Hybrid Case 1	94%	82%	104%	104%	<b>8%</b>
Hybrid Case 2	100%	85%	119%	120%	<b>14%</b>
Hybrid Case 3	97%	82%	103%	103%	<b>7%</b>
Hybrid Case 4	97%	87%	106%	106%	<b>7%</b>
Hybrid Case 5	99%	85%	110%	110%	<b>9%</b>
Hybrid Case 6	96%	83%	107%	107%	<b>9%</b>
Hybrid Case 7	100%	87%	110%	110%	<b>8%</b>
<b>Average</b>	<b>97%</b>	<b>82%</b>	<b>108%</b>	<b>108%</b>	

*Table of overall changes due to decrease in detection chance*

Sensitivity varied based on both the case being simulated and the output being analyzed. The threat detection function was the least sensitive to the change in detection probability, while the fault prevention function was the most sensitive. The Hydrophone, Wave Glider and Hybrid Case 2 were the most sensitive to the change, while Hybrid Case 3, 4 and the AIS case were the least sensitive. Nearly all changes were less than the amount the detection probability decreased, though the exact relationship would require additional analysis to determine.

### C. Sensitivity on message efficacy

The next major assumption was the efficacy of the warning messages to prevent faults. This is a major part of the TCPS and the only function that directly works to prevent damage to the cable system. However, since this system does not exist yet, estimates had to be made on the efficacy of the messages to prevent faults from occurring. Message efficacy also varies based on what type of sensor identified the threat. If detected by AIS, the TCPS will exact information on the threat and a direct line of communication, increasing the chance a warning message can prevent a cable fault. If detected by other sensors, the TCPS must use open VHF channels to communicate the warning message, reducing the chance the threat will receive the message.

	Initial Sim	Sensitivity Analysis
AIS	0.5	0.25
Hydrophone	0.25	0.1
SAS	0.25	0.1

*Table of probability of message success based on detection type*

For the sensitivity analysis, we lowered the message success probability from 50% to 25% for AIS, and from 25% to 10% for other sensors.

	Threats Detected				Difference	
	50/25% Messages		25/10% Messages		Detected	%
	Detected	%	Detected	%		
<b>As-Is</b>	<b>0</b>	<b>0</b>	0.0	0%	0.0	0%
AIS	14.0	21%	13.9	21%	-0.1	99%
HUGIN	7.5	11%	7.5	11%	0.0	100%
SeaGlider	7.2	11%	7.2	11%	0.0	100%
Hydrophone	61.7	92%	61.5	92%	-0.1	100%
Wave Glider	49.6	74%	49.6	74%	0.0	100%
Hybrid Case 1	20.3	30%	20.2	30%	-0.1	99%
Hybrid Case 2	61.5	92%	61.6	92%	0.1	100%
Hybrid Case 3	23.5	35%	23.4	35%	-0.1	100%
Hybrid Case 4	30.2	45%	30.2	45%	-0.1	100%
Hybrid Case 5	42.4	63%	42.5	63%	0.1	100%
Hybrid Case 6	34.6	52%	34.4	52%	-0.2	100%
Hybrid Case 7	44.2	66%	44.3	66%	0.1	100%

*Table of threat detection change for reduced message success probability*

Reducing the effect of the warning messages had no meaningful effect on the threat detection rates.

	<b>Faults Prevented</b>		<b>Faults Prevented</b>		<b>Difference</b>	
	<b>50/25% Messages</b>		<b>25/10% Messages</b>			
	Prevented	%	Prevented	%	Prevented	%
<b>As-Is</b>	0.00	0%	0.00	0%	0.0	0%
AIS	0.58	13%	0.42	9%	-0.2	72%
HUGIN	0.15	4%	0.07	2%	-0.1	47%
SeaGlider	0.19	4%	0.10	2%	-0.1	52%
Hydrophone	2.37	53%	1.49	34%	-0.9	63%
Wave Glider	1.98	45%	1.42	32%	-0.6	71%
Hybrid Case 1	0.71	16%	0.49	11%	-0.2	69%
Hybrid Case 2	2.45	56%	1.65	38%	-0.8	67%
Hybrid Case 3	0.92	21%	0.62	14%	-0.3	68%
Hybrid Case 4	1.23	28%	0.92	21%	-0.3	74%
Hybrid Case 5	1.73	39%	1.20	27%	-0.5	70%
Hybrid Case 6	1.49	34%	1.11	25%	-0.4	75%
Hybrid Case 7	2.02	45%	1.55	35%	-0.5	77%

*Table of changes to faults prevented due to reduction in message*

Reducing the probability of message success had a significant negative effect on faults prevented. AIS, Wave Glider and the Hybrid cases (which all include AIS) were the least affected, but the faults prevented for those cases were still reduced by over 20%. The HUGIN case was most affected, only preventing 47% of the faults it had previously prevented.

**Costs**

**50/25% Messages**

**25/10% Messages**

**Difference**

	Downtime	Total Cost	Downtime	Total Cost	Downtime	%	Total Costs	%
<b>As-Is</b>	1330	\$101,000,000	1330	\$101,000,000	0.0	100%	\$0	100%
AIS	1150	\$87,800,000	1200	\$91,600,000	50.0	104%	\$3,800,000	104%
HUGIN	1270	\$96,800,000	1290	\$98,200,000	20.0	102%	\$1,400,000	101%
SeaGlider	1260	\$96,400,000	1300	\$99,300,000	40.0	103%	\$2,900,000	103%
Hydrophone	620	\$47,200,000	870	\$66,200,000	250.0	140%	\$19,000,000	140%
Wave Glider	740	\$56,200,000	890	\$67,700,000	150.0	120%	\$11,500,000	120%
Hybrid Case 1	1100	\$84,000,000	1180	\$90,100,000	80.0	107%	\$6,100,000	107%
Hybrid Case 2	580	\$44,000,000	810	\$61,900,000	230.0	140%	\$17,900,000	141%
Hybrid Case 3	1060	\$80,500,000	1140	\$86,700,000	80.0	108%	\$6,200,000	108%
Hybrid Case 4	950	\$72,700,000	1060	\$80,900,000	110.0	112%	\$8,200,000	111%
Hybrid Case 5	790	\$60,400,000	970	\$73,900,000	180.0	123%	\$13,500,000	122%
Hybrid Case 6	890	\$67,600,000	980	\$74,400,000	90.0	110%	\$6,800,000	110%
Hybrid Case 7	730	\$55,500,000	860	\$65,500,000	130.0	118%	\$10,000,000	118%

*Table of costs and downtime changes due to decreased message efficacy*

Reducing message efficacy had a strong effect on costs and downtime as well. The Hydrophone and Hybrid 2 cases are most affected, increasing their downtime and costs by 40%. The HUGIN and SeaGlider cases were least effected, increasing their downtime and costs by a few percent only. Considering the probability of message success was reduced by 50% for AIS and reduced by 60% for Hydrophone and SAS, these large drops are to be expected, especially from those cases that rely heavily on non AIS sensors.

However, even with reduced prevention ability, TCPS cases are still able to prevent a significant number of faults incidents and reduce costs by millions of dollars. The TCPS also provides benefits due to identification of threats and reduction of repair time as well.

### Change due to decrease in message efficacy

	Threats	Faults	Downtime	Costs	Average
AIS	99%	72%	104%	104%	<b>9%</b>
HUGIN	100%	47%	102%	101%	<b>14%</b>
SeaGlider	100%	52%	103%	103%	<b>14%</b>
Hydrophone	100%	63%	140%	140%	<b>29%</b>
Wave Glider	100%	71%	120%	120%	<b>17%</b>
Hybrid Case 1	99%	69%	107%	107%	<b>12%</b>
Hybrid Case 2	100%	67%	140%	141%	<b>28%</b>
Hybrid Case 3	100%	68%	108%	108%	<b>12%</b>
Hybrid Case 4	100%	74%	112%	111%	<b>12%</b>
Hybrid Case 5	100%	70%	123%	122%	<b>19%</b>
Hybrid Case 6	100%	75%	110%	110%	<b>12%</b>
Hybrid Case 7	100%	77%	118%	118%	<b>15%</b>
<b>Average</b>	<b>100%</b>	<b>67%</b>	<b>116%</b>	<b>116%</b>	

*Table of overall changes due to reduction in message efficacy*

Threat detection is not sensitive to changes in message success. Fault prevention is sensitive, but not by as much as the probability was reduced – a 50% reduction in success rate led to only a 33% reduction in fault prevention. Costs and downtime both increased by 16% much less than might have been expected with the large drop in fault prevention.

#### *D. Overall Sensitivity results*

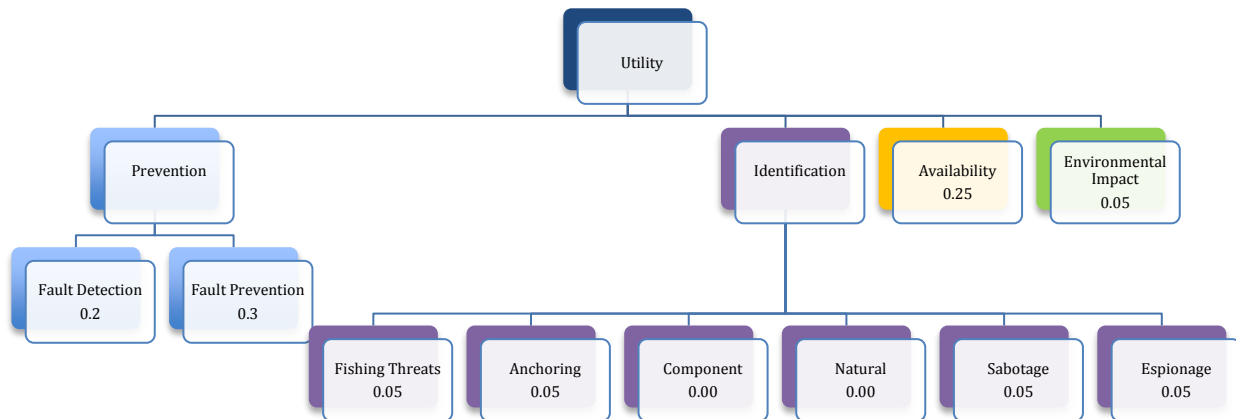
Overall the threat detection function was fairly insensitive to the changes. This is likely due to multiple chances a given TCPS agent may have to detect a threat. With the reduced probability of detection, agents will take longer to identify a threat, but will still be able to identify most threats before they leave the cable are.

The fault prevention function was the most affected by the changes, being reduced an average of 18% when the sensor probability was lowered, and reduced by 33% when the message success rate was reduced. Importantly, even at low success rates, the TCPS was still able to prevent some faults and reduced costs significantly from the As-Is case.

## 7.8 Validation

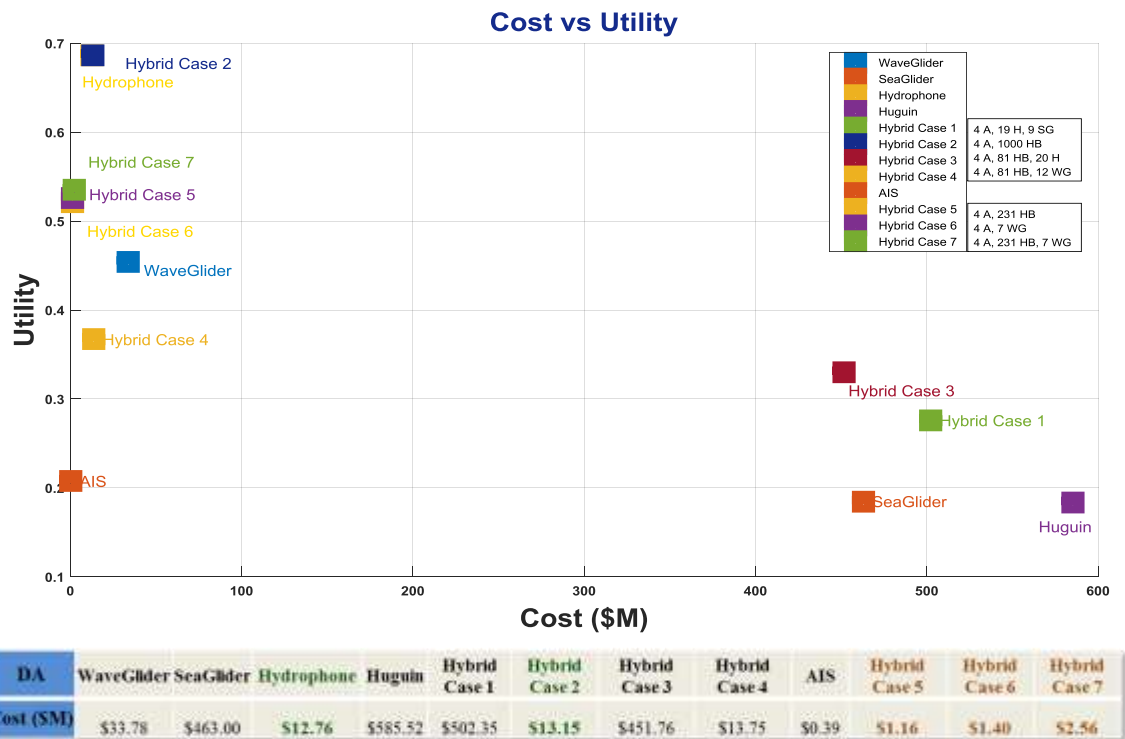
The approach to the validation of our simulation model consists of two parts: the validation of the “as-is” simulation model and the validation of the simulation model containing the design alternatives of the TCPS system. For the “as-is” simulation, the output results can be compared to the data that we have acquired through our research of current the fault statistics. As shown above, the as-is scenario closely correlates with the data gathered statistics. 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.

## 7.9 Utility



The utility for the outputs of the simulation were calculated using a hierarchy of measures derived from the stakeholder analysis and sponsor recommendations. However, the direct owners of the SEA-US cable were unreachable and their operational data is proprietary. Therefore, in order to conduct the analysis, sample weightings were placed based on estimations, with the intention that they could be, easily, changed as and when the system is employed by the owners. The hierarchy, shown above, consists of four major categories that were considered for each design alternative. All of the measures were computed on a linear scale of 0-100% The first category, prevention, consists of fault detection percentage and fault prevention percentage, both of which were calculated as the number of detected/prevented threats over the total number of

faults generated. The second category, identification, is composed of the percentage detected of each type of threat that could be generated. Since the natural threats (earthquakes, volcanoes, etc.) cannot be prevented, the weighting for that measure is set to 0. The availability measure is a combination of the minimum lifespan of a design alternative and the MTBF. The MTBF was evaluated as the percentage change in the MTBF output for a particular design alternative with respect to the as-is simulation output. The lifespan is defined as the total duration of time a design alternative can be in use before it must be replaced or significantly repaired. Based on our contact with the manufacturing companies, all of the components included had a tested lifespan of over 5 years, the projected lifecycle of our system, or the data was unavailable, therefore, maximum weighting was given to each one. The measure is still included in order to accommodate any future design alternatives that may come into the market as the system becomes employed. Similarly, data did not exist on the environmental impact of the active and passive technologies. Therefore, a maximum weighting was given to all of them as they would not impact the outcome of the utility until further information is revealed. One of the objectives of the simulation and utility analysis, which will be discussed further in the business case, is to become the preliminary product of the system and to increase its accuracy through each iteration. After each subsequent cable is analyzed and a design alternative is implemented, the data gathered from its operation can be used to refine our simulation models and utility breakdown. Therefore, starting with measures that have no impact on the utility for the first cable, ensures that the simulation and analysis is flexible enough to accommodate future refinement.

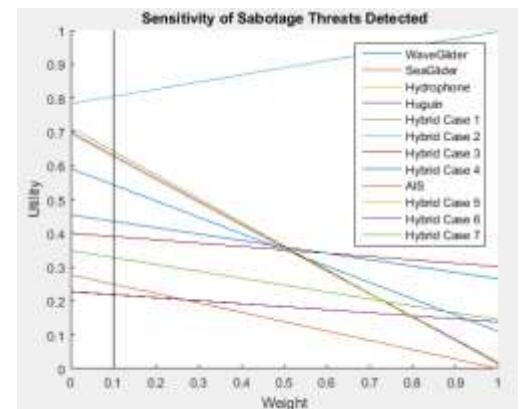
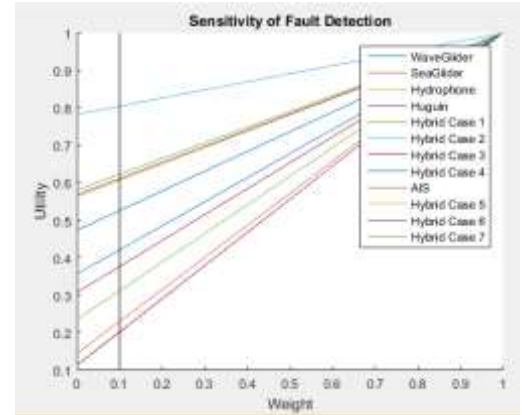
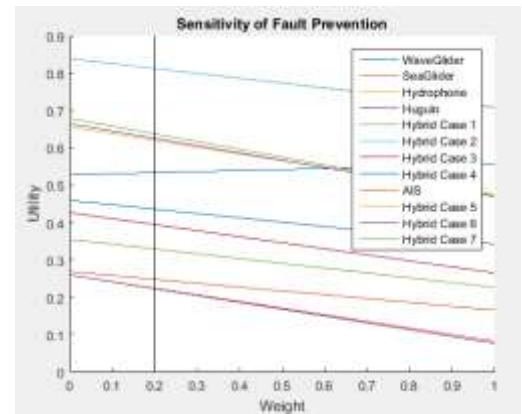
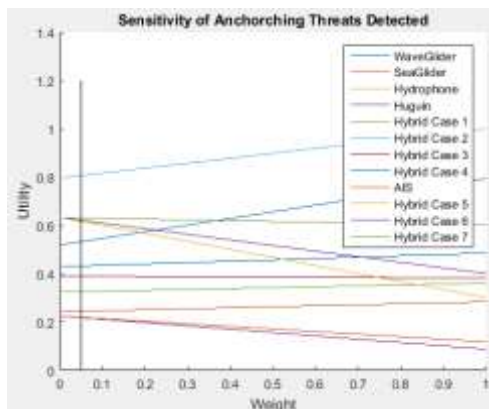
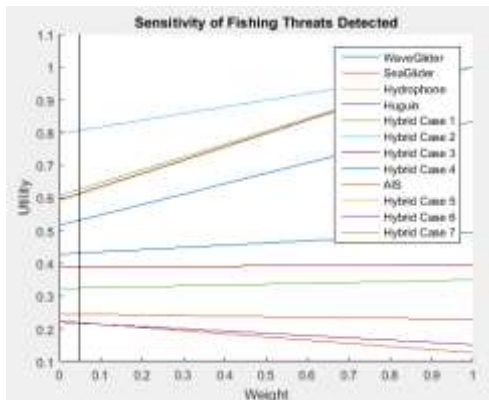


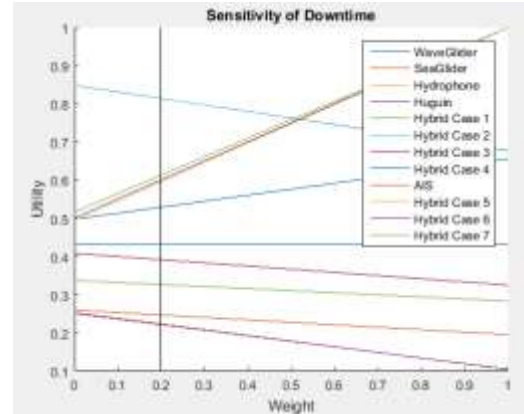
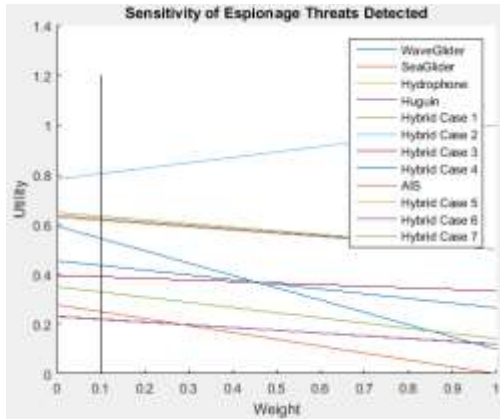
The overall utility for a design alternative is the sum of each individual utility measure times the scaled output value from the simulation. The cost vs utility chart shown above,

generated in MATLAB R2015a, shows the comparisons of the utility of the design alternatives vs their costs. The highest utility alternative is the hydrophone only case with full coverage followed closely by the hybrid case 2 (AIS & Hydrophone), also with full coverage. The alternative with the highest utility-cost ratio is Hybrid case 5, which is a partial coverage case consisting of hydrophones and the AIS system. In a scenario where the downside of a security risk is the loss of operation, the highest utility-cost ratio design alternative may not be the one chosen and the stakeholder could end up choosing the one with maximum utility. Given this reality, it is important to note that the large variation in coverage and cost ends up serving the customer's needs better by providing more choices to suit their particular cable.

### Sensitivity of Weightings

Sensitivity of the measures was tested by iteratively incrementing the weightings from 0-1.0 and computing the utility of the design alternatives. The charts shown are the sensitivity of the measures that had an impact on the overall utility of a design alternative. The vertical black line indicates the current value of the measure. If a design alternative's utility changes within a 0.1 range, it was considered sensitive. The results of this analysis are that the alternatives are not very sensitive and there is no change in the utility ranking if the weightings were changed by 10%.





### Recommendations

Based on the cost vs utility and the sensitivity analysis, if a design alternative had to be chosen for the SEA-US cable without further stakeholder input, the TCPS team recommends the Hybrid Case 5 which consists of 4 AIS nodes at 4 CLS stations, 4 CODTR machines, and 231 hydrophone buoys placed along the length of the cable at approximately 32% coverage. This would cost 1.16 million dollars, not including a mission control center, and provide a utility of greater than 0.5. However, as will be mentioned in the business case analysis, the implementation of such a system would require the operation of a mission control center. This would most feasibly be done by an independent entity that contracts with the cable companies. As such, the independent entity would be able to procure confidential information regarding the cable operation and history, at no risk to the owner, therefore, the utility and recommendation would be subject to changes.

## 8.0 Business Case Analysis – Cable Shield

### 8.1 Business Model

As mentioned throughout this report, the undersea fiber optic cable network is a multibillion-dollar industry that is growing 36% annually. This critical infrastructure is vital to all facets of society today. There are hundreds of millions of dollars of preventable losses each year, which presents an opportunity for TCPS to be analyzed as a viable business. The mock company developed for this analysis is called Cable Shield.

The analysis in this section was done to show the impact of Cable Shield on the current market as well as its earning potential as a business. Due to the inability to retrieve accurate cost information for underwater technology due to the competitive nature of the manufacturers as well as other items, several assumptions were made in order to get a result from our model. The cost model can easily be updated with real cost information. This analysis will also show the low startup costs in comparison to the high earning potential of the proposed system.

The business model that Cable Shield will be implementing is an annual subscription model that can be tailored to the customers needs. The flexible design of TCPS will allow for highly scalable systems and the ability to expand quickly to more cable systems. The scenario used for this analysis is done on the SEA-US cable system, which crosses the Pacific Ocean and connects California, Hawaii, Guam, and the Philippines. This analysis can be done on any cable system, but will have different results based on cable length, number of cable landing stations (CLS), and desired coverage by the customer.

## 8.2 Market Strategy and Prospective Market

Based on the Context and Stakeholder Analysis, we have identified potential customers that would benefit from Cable Shield systems. The following table shows an example of the various types of customers and the benefit they will be receiving.

<b>Customer</b>	<b>Benefit</b>
TE Connectivity (Individual Cable Owners)	Value more cable uptime
Global Cloud XChange (Individual Cable Owners with history of faults)	History of espionage, value cable uptime
Cable Repair Companies	Fault data and type to expedite repair process
Governments (NSA, Military)	Concerned with hostile threat identification
Google	Value cable uptime and fault prevention
Verizon, AT&T	Value cable uptime

The Market Strategy for Cable Shield consists of a three-stage process for entry into the market. The purpose of this is to start with a low cost method of gaining customers before implementing the different design alternatives mentioned in the Simulation section.

### 1. Stage 1: Optimized Recommendations

The first stage will consist of Cable Shield consulting with telecommunication companies and cable owners and providing them optimized recommendations for the best protection of their cable using Cable Shield’s analytics software, C<sub>3</sub>PO (Comprehensive Coordinated Cable Protection Optimizer), which is discussed in detail in the Simulation section of this report. These recommendations will include optimal agent locations (Hydrophones, AUVs, AIS, etc.) and specifications based on history, big data analytics, and forecasting. The total cost of alternatives and agents will also be provided, which will vary based on the desired coverage of the customer. Because C<sub>3</sub>PO is highly scalable software, Cable Shield can provide multiple coverage rates to display to the potential customer. Lastly, the recommendation will identify high-risk locations for cable faults. When the customer decides to subscribe to Cable Shield, Stage 2 will begin.

2. *Stage 2: Build Mission Control*

Upon receiving revenue generated from Stage 1, Cable Shield will begin construction of Mission Control, which is explained in the Operational Concept section. The purpose of waiting to gain one customer prior to building Mission Control is to ensure that Cable Shield will recoup the nonrecurring costs of Mission Control and the costs of the agents. Mission Control will be stood up in 6-12 months. Once Mission Control is in place, Cable Shield will install the agents at the specified locations near the cable. At the completion of that task, Cable Shield will begin its monitoring service for the customer. Cost estimates for this process will be shown later in this section.

3. *Stage 3: Economies of Scale*

Stage 3 is where Cable Shield will produce a majority of its revenue due to the use of economies of scale. Because Mission Control (Stage 2) will only need to be built once, more subscriptions to Cable Shield will cover the recurring costs of Mission Control and the agents. All cable monitoring will take place inside Mission Control, eliminating the need for multiple locations for each cable. The last step in Stage 3 is to use Mission Control to record data collected from the agents. Using this historical data, Cable Shield will be able to improve its protection system in order to outperform any competitors.

**8.3 Cost**

Costs for starting up Cable Shield are broken down into recurring and nonrecurring costs for the following sections: Labor, Cable costs, and Mission control costs. As mentioned prior, precise cost information was not obtained in most cases, so best engineering judgment was used in those cases. The table below shows the total costs for Cable Shield, with breakdowns shown in subsequent tables.

<b>Total Costs</b>			
<b>Mission Control</b>		<b>Per Cable</b>	
Nonrecurring	Recurring	Nonrecurring	Recurring
<b>\$1,350,000</b>	<b>\$1,120,000</b>	<b>\$1,300,000</b>	<b>\$58,000</b>

Mission Control Breakdown:

<b>Mission Control Yearly Labor Cost</b>
--

Systems Admin	\$100,000
4 Managers	\$300,000
5 Monitoring Staff	\$250,000
2 Specialty Hires	\$200,000
Consultants	\$100,000
<b>Total</b>	<b>\$950,000</b>

<b>Mission Control Capital Costs</b>		
	Nonrecurring	Recurring
Building	\$500,000	\$60,000
Software	\$500,000	\$100,000
Communication	\$100,000	\$5,000
Servers	\$250,000	\$5,000
<b>Total</b>	<b>\$1,350,000</b>	<b>\$170,000</b>

Cable Shield will need to make several hires to help develop and run Mission Control. The System Administrator will assist in the data collection and signal processing of Mission Control. The 4 managers will include a CEO (Dane Underwood), CTO (Kumar Karra), COO (Isaac Geisler), and CFO (Felipe Cardenas). Monitoring staff members will keep 24-hour watch on the cable systems and processors inside Mission Control with rotating shifts. Specialty Hires will include a technology expert in software engineering and an expert in contract and legal management. Lastly, Cable Shield will employ consultants for business development and marketing.

For Mission Control, costs will include building, materials, and communication. Building of the Mission Control Center is estimated to be a high upfront cost, with recurring costs to cover maintenance, upgrades, and payments. Software costs are relatively high and will include signal and data processing software. Communication costs cover secure Internet and satellite connections. Lastly, due to the immense amount of data gained from the agents in the ocean, multiple servers will be needed.

Cable Breakdown (will vary depending on cable length, CLSs, and desired coverage):

<b>Cost per Cable</b>		
	Nonrecurring	Recurring
Monitoring Agents	\$500,000	\$50,000
CODTR (2)	\$800,000	\$8,000
<b>Total</b>	<b>\$1,300,000</b>	<b>\$58,000</b>

Monitoring agents' nonrecurring cost may vary from cable to cable, but the estimate for the SEA-US cable is shown in the table. Due to the long lifecycle of the monitoring agents, maintenance and other recurring costs are relatively low. Coherent Optical Time Domain

Refractometer (COTDR) will be used at cable landing stations. Though there is a high initial cost for the COTDR, it will significantly increase the ability to locate the location of a cable fault, thus decreasing the repair process time and increasing availability of the cable system.

### 8.4 Sales Profile

When selling the protection system to customers, Cable Shield charge an annual price of cost plus 20% per cable per year with a 5-year monitoring contract. For the SEA-US Cable, which is 15,000 km long and has 4 CLSs, the annual subscription price for the full coverage Hybrid 2 system (Hydrophones, AIS and COTDRs) will be \$1,630,000 per year.

### 8.5 Return On Investment

Calculations for Return On Investment (ROI) included both a pessimistic and optimistic case for the projection of Cable Shield as a business. The initial investment needed for the start up of Cable Shield is shown:

$$\text{Initial Investment} = \text{Mission Control Nonrecurring Cost} + 1 \text{ Year Operating Expenses} = \$2,368,000$$

For the pessimistic case, it is assumed that one cable will be protected in the first year of operation with *one* new cable protected every *two* years. Over a 10-year period with this rate of market penetration, Cable Shield will see a **230%** ROI in 10 years and break even in two years.



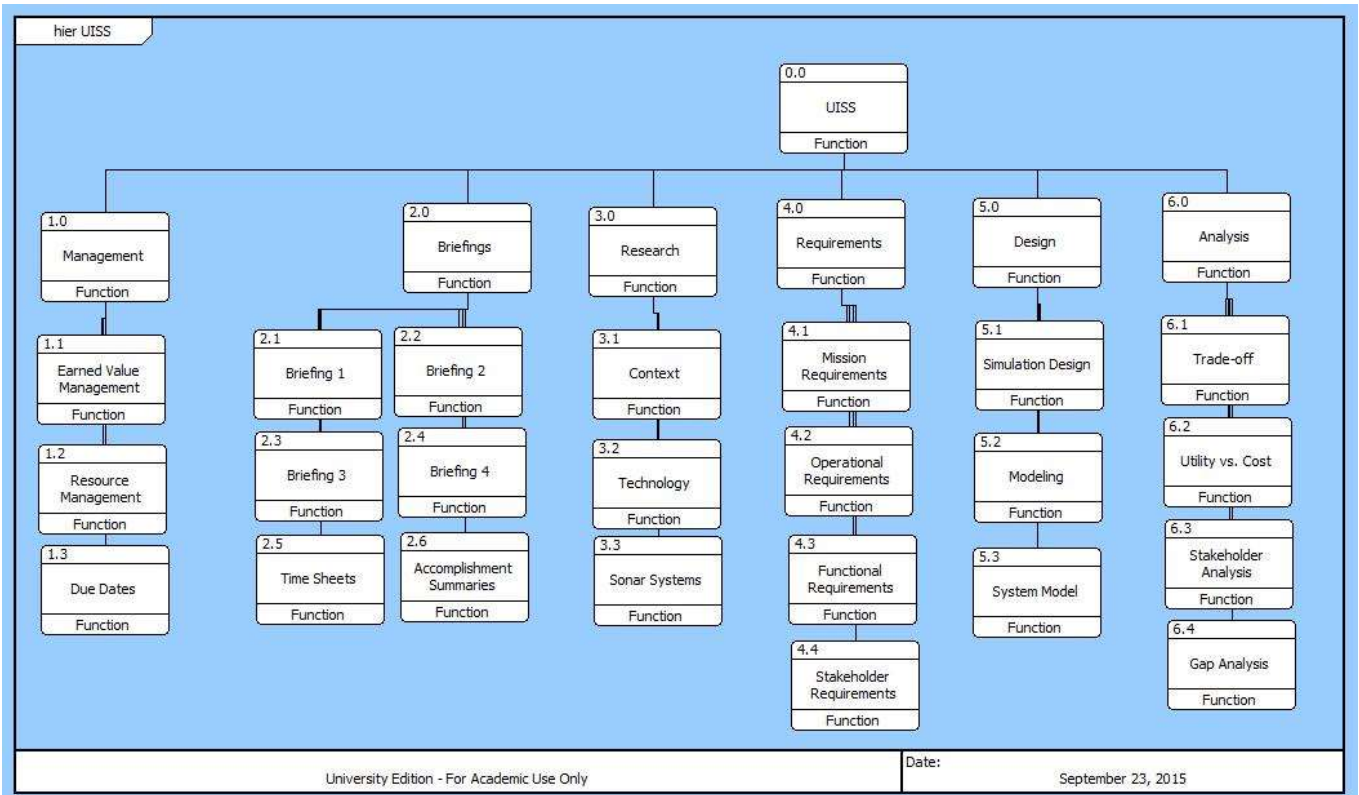
For the optimistic case, it is assumed that one cable will be protected in the first year of operation with *two* new cables protected every year. Over a 10-year period with this rate of market penetration, Cable Shield will see a **1130%** ROI in 10 years and break even in one year.



## 9.0 Project Plan

### 9.1 Work Breakdown Structure

The following hierarchy shows the levels at which we have decomposed all parts of the project. Categories were based upon deliverables and important tasks needed to complete the project. A detailed WBS with each task is provided in the Appendix.



Management is our first breakdown because it is the most important aspect of the project. Within management, we will be monitoring our progress on the project, assigning tasks, and tracking our CPI and SPI.

Briefings include all major briefings, ultimately leading up to the faculty presentations on November 20<sup>th</sup>. Time sheets and Accomplishment Summaries are also listed because they are due weekly and help us collaborate on new findings or completed tasks in the project.

Research was a significant component during the first several weeks of the project, especially when researching context and alternatives. We are continuing to research better data for simulation and also continuing to research current events and news about recent cable damages.

Requirements are next and include Mission, Functional, Design, and Simulation requirements. These are important for determining the success of the system and informing stakeholders what TCPS will do and how TCPS will accomplish the task.

We are currently diving into the Design phase. This part will consume a majority of our efforts for the remainder of the project. As mentioned in the Simulation section, we have determined how we are going to model the system, but are in the process of writing the program.

Analysis will be another significant part of the project, as it will include recommendations for the most optimal system. We will do this by creating a utility function and performing a trade-off analysis. We anticipate beginning this phase in December and continuing to develop it during the Spring semester.

## 9.2 Schedule

The project schedule was derived from our WBS and deliverable due dates. Instead of taking a waterfall approach and completing one task at a time, we are implementing a cyclical approach. We are doing this by dividing the project into phases. Each phase is centered on the project briefings. There are certain tasks that need to be accomplished prior to each briefing. After we receive feedback or find new information, we scheduled a time where we will revisit our tasks and make adjustments as needed. We felt this method would make sense because we will be continuously improving on the project throughout the course of the year.

## 9.3 Critical Path

Most of the tasks that were in the initial phases of the project were set to have a specific deadline, mainly project deliverables. As a result, almost all of the tasks had a slack time and, therefore, were not included in the critical path. Since the later phases did not have a specified deadline, due to the uncertainty in competition dates, the following is a list of those task groups that are included in the critical path.

# CRITICAL TASKS



- Status: Complete
- Status: On Schedule
- Status: Late
- Status: Future Task

A task is critical if there is no room in the schedule for it to slip.  
[Learn more about managing your project's critical path.](#)

Name	Start	Finish	% Complete	Remaining Work	Resource Names
Practice Presentation	Sat 10/24/15	Sun 10/25/15	0%	4 hrs	Dane,Felipe,Isaac, Kumar
[Phase 11] Briefing 1 R&U	Sat 1/30/16	Fri 2/12/16	0%	150 hrs	Dane,Felipe,Isaac, Kumar
[Phase 12] Work for Briefing 2 495	Fri 2/12/16	Thu 2/18/16	0%	75 hrs	Dane,Felipe,Isaac, Kumar
[Phase 13] Work for Briefing 3	Thu 2/18/16	Thu 3/10/16	0%	250 hrs	Dane,Felipe,Isaac, Kumar
[Phase 14] Conference Prep	Thu 3/10/16	Thu 3/31/16	0%	250 hrs	Dane,Felipe,Isaac, Kumar

## 9.4 Budget

The project budget was developed based on several assumptions. First, we are assuming a 20-hour workweek for each team member. We felt that this was a reasonable assumption to make because the amount of time spent on this project will be close to that number on any given week.

We also decided on this number for the sake of simplicity when calculating SPI and CPI in Microsoft Project.

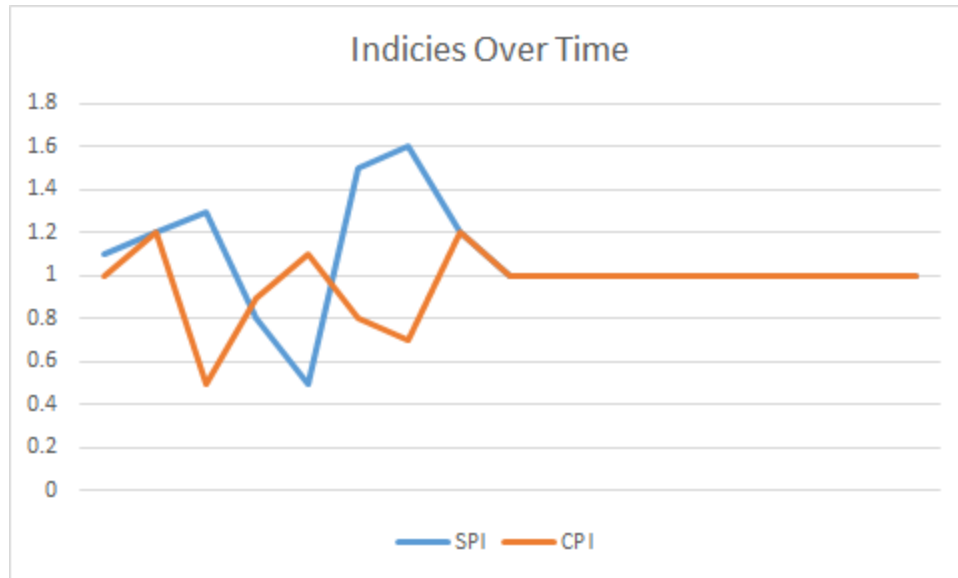
Our team will be charging an hourly rate of \$60 per hour. The average starting salary for a Systems Engineer in the Washington, D.C. area is \$70,000, which equates to roughly \$30 per hour. We are implementing a 1:1 direct to indirect cost ratio on our hourly rate. This returns a \$60 per hour rate. The following table shows our planned costs for the duration of the project.

	Individual Total (9/13-5/13)	Team Total (9/13-5/13)
Planned Time (Hours)	623.8	2495.2
Planned Value (PV)	\$37,428	\$149,712

*Figure 7.1 – Planned Time and Costs*

**9.5 Earned Value Management**

The SPI and CPI have been fluctuating over and under 1.0 as a result of the initial uncertainty regarding the scope of the project as well as the time/cost estimation of the earlier tasks. However, over time, we expect the SPI and CPI to stabilize given the maturity of the project along with having prior tasks as guidelines for estimating the duration of future tasks.



Expected Value	Actual Cost	Variance
\$135,880	\$149,712	\$13,882

The following Gantt chart shows the overall project plan as broken down into 14 phases, where each phase, after phase 1, includes a review and update period in order to makes improvements on previously completed tasks.



## 9.6 Project Risks and Risk Mitigation

Risk Mitigation is performed using the FMEA matrix.

<b>Risk</b>	<b>S</b>	<b>L</b>	<b>D</b>	<b>RPN</b>	<b>Mitigation</b>
<b>Critical Tasks:</b> Failure to complete tasks in critical path on time can delay project.	9	8	5	360	Start early and allot extra time for critical tasks.
<b>Requirements Inflation and Unexpected Scope Expansion:</b> Project scope becomes too large. Constant changes in requirements and scope can cause delays and costs.	8	8	5	320	Have weekly meetings to ensure project is still in scope and progress is made. These meetings will allow the project manager to have an idea of where the project stands and perform trade-off analysis to accommodate the revisions.
<b>Misspecification and Errors:</b> Provide the wrong solution. Solution contains errors or unneeded recommendations.	10	5	5	250	Team members meet weekly to discuss progress of project and hold each other accountable. Work must be done in a timely manner to allow time for revisions.
<b>Simulation:</b> Team members do not have plenty of experience in simulation. Sensitivity and trade-off analysis depends on simulation.	9	5	5	225	Set objectives before simulation begins to clarify goals of simulation. Research thoroughly beforehand. Start before Fall semester ends and work through winter break.
<b>Background Information:</b> Data regarding underwater cables are confidential and/or incomplete. Some information obtained are estimates.	8	7	3	168	Use open source data and sensible estimations.
<b>Stakeholders:</b> Satisfying stakeholder objectives might become infeasible	8	5	3	120	Justify solution by achieving stakeholder's feasible objectives.
<b>Communication with Sponsor:</b> Sponsor can be busy and difficult to reach.	3	5	6	90	Allow ample time for sponsor to respond.

**Severity (S):** 1(less severe) - 10 (very severe)

**Likelihood (L):** 1 (less likely to occur) - 10 (almost certain to occur)

**Detection (D):** 1 (able to detect before problem)-- 10 (almost unable to detect before it occurs)

## Sources

- [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\\_IViko](http://www.maltatoday.com.mt/news/national/13804/damaged-go-submarine-cable-repaired#.Vhkz3_IViko)
- [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](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](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](http://www.nec.com/en/global/solutions/safety/critical_infra/harbormonitoring.html).
- [26] "Autonomous Underwater Surveillance System Network," L3 Oceania, 2014. [Online]. Available: [http://www2.l-3com.com/oceania/products/maritime\\_aussnet.htm](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](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](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.