EVALUATING RESILIENCE OF OIL AND GAS CYBER PHYSICAL SYSTEMS: A ROADMAP

Yatin Wadhawan
University of Southern California
Los Angeles, USA
ywadhawa@usc.edu

Dr. Clifford Neuman
ISI, University of Southern California
Los Angeles, USA
bcn@isi.edu

ABSTRACT
Cyber attacks affect not only online profiles, bank accounts, and medical health records but also physical infrastructure including oil and gas, the power grid, nuclear, and water treatment plants. A stable energy supply is essential for economic prosperity. According to US Department of Homeland Security [12], approximately 22% of electricity is produced by natural gas combustion. A recent cyber attack on Norwegian Statoil [15] increased concerns regarding the safety of such critical infrastructure. In this research paper, we describe a function-based approach and framework for evaluating the resilience of oil and gas cyber-physical systems (O&GP) under cyber attack. We discuss use of the Measurement-Algorithm-Control system model for simulating extreme and rare events in O&GP. We describe ongoing research for which we are in the data collection phase.

Keywords
Cyber-Physical Systems (CPS), Information Security, Oil, Gas, Control Systems, Modeling, Simulation, Natural gas, Pipeline, Oil and Gas Plant (O&GP), Function based approach, Cyber Security (CS), Remoter Terminal Unit (RTU)

1. INTRODUCTION
Our nation's prosperity is highly dependent upon the energy sector. The energy sector serves hospitals, transportation, public networks, business, production of energy, production of goods and more. A failure of an operation in industrial control systems can have cascading effects on different sectors of the economy. A single cyber attack can cause a huge loss to the US economy in terms of money and utilities. According to Lloyd's Emergency risk report of 2015 [16], a major cyber attack on the U.S. electric grid could cause over a $1 trillion in economic impact and $71.1 billion in insurance claims. It is imperative to understand these infrastructures and develop strategies and policies to protect them.

According to the US Department of Homeland Security [12], the energy sector is divided into three highly interdependent segments: electricity, petroleum and natural gas. Natural gas fuels many electric plants that generate electricity; on the other hand, components of a natural gas plant require electricity for operation. A failure of a function in either can have cascading effects on other systems. Most researchers have focused on industrial control systems such as the Smart Grid and performed experiments in that domain. No one has performed detailed research on security of O&GP cyber physical systems. In this research paper, our focus is to describe an approach to evaluate the resilience of the O&GP under cyber attacks. It is paramount to understand the system components and how it works before performing analysis.

1.1 Overview of Oil and Gas Production
O&GP is divided into 3 major sectors: upstream, midstream and downstream. Upstream refers to exploration and production, midstream refers to the transportation and downstream refers to refining and distribution of products of oil and gas. In this study we have narrowed our focus on oil production and distribution via pipelines. Exploration and drilling are out of the scope of this research. Production of oil and gas includes pumping, storage, well maintenance, monitoring, pipeline distribution [9] and post production involves distributing it to the end customer, capping of the sea well and water quality management if offshore.

According to US Environmental Protection Agency [11], "Natural gas is formed when layers of buried animals, plants and gases are exposed to intense heat and pressure over thousands of years." Steps of producing the natural gas [10] are: (1) take the gas from the well heads, (2) condensate and remove water, (3) acid gas removal, (4) dehydration, (5) mercury removal, (6) nitrogen rejection using cryogenic process, (7) NGL recovery, (8) fractionation train and (9) sweeting units. By-products of Natural gas are water, propane, butane, pentanes, and sulphuric acid. The oil production plant begins after Sucker rod pumps take the oil from the ground or seabed (if offshore). The oil is routed to the separator, which will separate oil, gas and water. The wet gas is produced which is saturated with water and liquid alkanes. The gas is routed through compressors and coolers, which will remove the liquids from it. The gas is compressed and exported via pipelines otherwise gas is flared if its export is uneconomical.

It is important to classify the O&GP as onshore and offshore [1]. Onshore is drilling deep holes under the earth surface where as offshore is drilling the holes under the seabed. Although in both the cases similar methods of drilling are used, e.g. horizontal, rotatory and directional drilling, since offshore drilling takes place at sea, it is paramount to provide security and resilience to perform drilling. Offshore drilling bears more risks to marine life; any disaster can lead to water pollution, which will destroy the marine habitat. Security of such system will differ from onshore depending upon the kind of SCADA system implemented and difference in variables, which may affect the resilience. The communication infrastructure changes when we deal with offshore. The offshore systems communicate via satellite. The corporate offices receive the readings of the field devices and controllers via satellite. We need to evaluate the resilience of the system in both scenarios. In this research paper, we have proposed a method of evaluating the resilience of the O&GP for onshore. Our future work will focus in offshore settings as well.

1.2 O&G Pipeline System
According to an American Petroleum Institute report of 2015 [17], the U.S. natural gas pipeline system consists of 305,000 miles of pipelines, moving natural gas to processing facilities and then to homes and factories throughout the country. Pipelines play a vital role in our daily lives. Air travel, vehicle transportation, cooking and the heating of places are all made possible by the fuels delivered via pipelines.

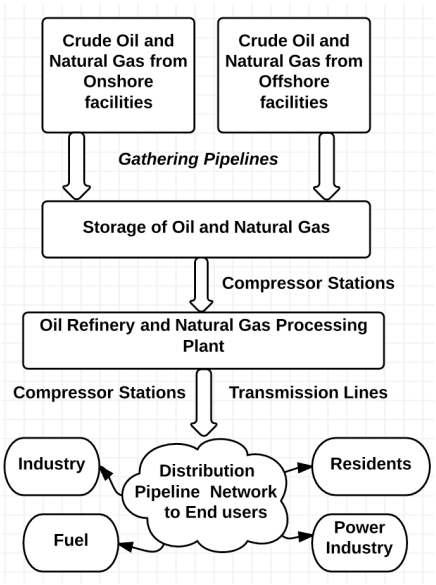


Figure 1. Oil and Gas Processing Flow

If this pipeline distribution is disturbed either maliciously or non-maliciously even for a small period of time, it can cause great loss to the economy. Thus it is important to evaluate the resilience of such system under cyber attacks. According to Argonne National Laboratory Report [9] on National Gas Pipeline Technology Review 2007, there are 3 major types of pipelines: (1) Gathering system, (2) Transmission system and (3) Distribution system. The gathering pipeline system is responsible for gathering raw oil/gas from the extracting units such as oil and gas wells. This system sends the raw material extracted to the processing plant. Once the oil/gas is processed, using Transmission pipeline system, they are transported thousands of miles across US. One can see in the figure 1 that from the transmission pipelines, many distribution pipelines are separated which provides oil/gas to the end points such as homes, manufacturing plants and other businesses through mains and service lines.

Raw oil/gas is extracted from the onshore and offshore facilities via gathering lines; it is transported to the processing plants. Once it is processed, transportation lines take it to distant locations and compressor stations are installed at intervals. We need to understand how compressor stations can be used to affect the resilience of the pipeline system. It is worth noting that many past attacks have targeted compressor stations with a goal of bringing the pipeline system down. According to the US Department of Homeland Security, ICS-CERT (Industrial Control System-Computer Emergency Readiness Team) received a report on February 22, 2013 [18] from a gas compressor station about an increase in brute force attempts to access its process control network and they found that about 70% of attacks targeted critical infrastructure organizations including the energy sector. In this way, the energy sector is targeted with a possible outcome for man-made environmental disaster. There are several attack vectors that can be used by an attacker to compromise the Industrial Control system (ICS) like O&GP. In order to understand those attack vectors, we need to understand O&GP as a Cyber Physical System (CPS).

1.3 O&GP as Cyber Physical System

In cyber-physical systems [6] such as O&GP, physical components are the physical plant and processes that are monitored and controlled by the cyber infrastructure of the system, which includes programmable logic controllers (PLCs), sensors, and SCADA. It is imperative to understand that critical machineries used in the O&GP have joint or separate control systems. Data about the properties of the gas such as temperature, pressure, density, and velocity of the oil/gas are given by sensors, which then fed into these systems to monitor the state. If the state of the system is not appropriate, automatic or manual commands are sent to change the state of the system. An engineer can send remote commands to increase the speed of the sucker rod pump up to certain level to extract more oil/gas from the oil well or seabed. The pressure of the gas is controlled by a system when it is passing through a pipeline system so that it does not leak or damage the pipeline walls. An engineer can send remote commands to intermediate compressors attached to the pipeline to compress the gas if he observes that gas is expanding.

With respect to the observation of gas properties, sensors are placed at locations to gather and send data to the control system, which applies computational algorithms to detect or predict anomalies. Once an anomaly is detected, appropriate control commands are sent to change the function of the physical infrastructure. A logic-based computer command can stop, start or change the parameters of the oil/gas compressors. Such network-integrated solutions are useful since one can change the state of the system remotely and quickly by sending a single command over the network. At the same time they are dangerous since they delegate trust in the underlying computer systems and network. What if a malicious attacker or a disgruntled employee others [4] with motive to harm a system controls it? We now discuss attack scenarios possible in O&GP CPS.

1.4 Cyber-Physical Attacks on O&GP

An activity performed in the cyber domain can affect the physical infrastructure or vice versa. There are different types of attack [6] scenarios.

1. Physical-Physical
2. Cyber-physical
3. Physical-Cyber
4. Cyber-cyber
5. Cyber-physical-cyber
6. Physical-cyber-physical

For an instance, if the system that controls and monitors (cyber) the pressure of the gas in the pipeline sends commands to change the pressure (decrease the pressure via decompressors: physical part) beyond the secure limits, this may allow the gas to leak or destroy the walls of the pipeline. This is an example of cyber-physical attack scenario. An example of physical-cyber-physical is for a person to take a match to fire sensor (Physical action), this will trigger a response and control system (cyber part) will take action to start water shower (physical action). We need to understand the functions that attackers can potentially target. What are those functions, what are the components that support that function, machinery, communication network and attack vector possible? These are some questions we need to address before describing how to protect and evaluate the resilience of the system.

1.5 Motivation of Our Approach

We have used function-based approach [3] in this research paper so that we can narrow our focus of to a specific function of the oil and gas plant and abstract the cyber attacks that may affect that function. For an instance, the function of pipeline system is to

distribute gas from production plant to end-users. We focus on this function and we answer questions such as: what are the components that affect this function, how those components are affected via cyber-physical attacks, what are the cyber attacks possible and what are the attack vectors used by attackers. It is a systematic way to drill down and understand how the resilience of the system is affected by disturbing a specific function.

There are several ways in which an attacker attacks the system; by abstracting all the attacks, which affect the particular function we can focus on evaluating the resilience of that function under various cyber attacks. For experimentation, we have adopted the approach of Measurement-Algorithm-Control system. The cyber physical system works in a closed feedback loop where sensors sense the state of the system and deliver this information to the control system, which further evaluates the overall state to check whether everything is working. If not, the control system sends commands to the actuators to change the state to an acceptable level. The algorithm implemented in the control system defines the actions for the corresponding state of the system. Our approach helps to evaluate the resilience of the system when a specific attack disturbs this feedback loop.

In this research paper, we describe the roadmap and a framework to evaluate the resilience of O&GP under cyber attacks. We begin with an overview of state of the art in section 2. We next propose the function-based approach in section 3, which abstracts all attacks to target a particular function. We follow with the description of various data points in section 4, which are essential part of our measurement model. We conclude by describing a model to perform simulation and our future research objectives.

2. RELATED WORK

SCADA stands for Supervisory control and data acquisition; it is a system that controls and monitors ICS such as O&GP. In [1] a comprehensive survey of O&GP SCADA systems is prepared to support an assessment of the current state of SCADA technology and to focus on reliability. The author described the generalized system architecture for O&GP and technology trends in the SCADA offshore. That research paper not only provided us the distinction between onshore and offshore O&GP but also evaluates the technology and reliability of these systems. There are 3 parameters described in [1] as a metric to evaluate the reliability:

1. Mean time between failures.
2. System Availability
3. Probability of facility damage

These metrics are important since they depict the resilience of the system under abnormal activities (malicious or non-malicious). The failure events such as sensor failure, communication network failures are critical since their effects can be cascading on other parts of the system. CPS requires real time data collection and analysis to detect and predict failures. The research paper [2] describes the security issues prevalent in the SCADA systems. Since systems like O&GP are controlled by SCADA systems, it is imperative to understand the weaknesses in the system. There is a need to improve several security functions in context of O&GP:

1. Access Control
2. Firewall and Intrusion Detection System
3. Key Management
4. Protocol Vulnerability Assessment
5. Device OS and Security

The function-based methodology used in [3] creates an attack tree, which targets a particular function. For instance, in the power grid the function one can choose is delivery of power. The question arises - what are the components responsible for power delivery, what is the attack vector that modifies the working of components, and how the resilience of the system is affected. We use a similar approach in our research but in the context of O&GP. There are a number of challenges for securing CPS [4,6].

In [4], the author talks about the actors who can attack the critical infrastructure (such as cyber criminals, disgruntled employees terrorist and nation states) and the difference between the IT security in corporate settings and IT security in CPS. It is important to narrow the focus on prevention, detection or resilience. On the other hand, the author in [6] describes the design methodology for developing a secure CPS architecture. It is important to define the authorized and unauthorized information and control flow and physical as well as cyber consequences of breach. The modeling of cyber physical interaction is essential for evaluating the resilience of the system.

A failure in the power grid can stop the functioning of the O&GP or vice versa because of the interdependence between these systems. Modeling and simulation [5] of interdependences in these systems can provide insights in the complex nature of their functions, behaviors and operational characteristics. The critical infrastructures are interdependent in 4 ways: Physical, geographical, cyber and logical. Such distinctions demonstrate that a change in one can bring the change in another. When we describe our resilience model for O&GP, by finding the interdependencies between O&GP and other systems, we learn how the effects of an attack on one system can harm another system's functionality.

In [7], the author described the importance of minimum state awareness of control system to maintain its resilience under cyber attack. The research paper describes the control theory and how a closed loop system including sensors, controllers and actuators works. An adversary can reduce the awareness of the system's state, which can reduce the overall resilience of the system. According to [1], real time state information is important so that controllers or administrators can take appropriate actions to change to valid state. This research paper inspires our model of Measurement-Algorithm-Control. After performing simulation, we will draw a line between acceptable and non-acceptable values of variables.

In order to perform the experiment, we need a testbed where we can design our system and simulate cyber-physical attacks. The research paper [8] describes testbeds such as Real time Immersive Network Simulation Environment (RINSE), which we will use as our experiment testbed. RINSE is equipped with industrial control equipment including sensors, network devices and PLCs. We will develop several layers in our testbed: Physical layer, sensors and actuators, layer of RTU, Wireless Mesh Network, Master System and Human Machine Interface (HMI). We will simulate the realistic behavior of the system under cyber attacks. We will maintain the state of the system and see how cyber attacks change that state and affect the resilience. The rest of the state of art we have drawn from the US department of Homeland Security, Department of Environment and Department of Pipeline which provides descriptions of pipeline and hazardous material [14] [9], Natural gas [10] [11] [13] and Oil production plant sources.

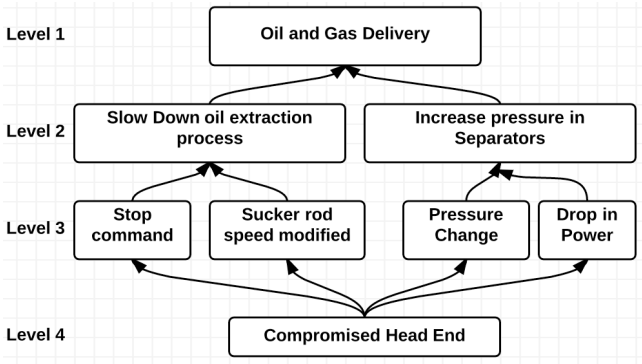


Figure 2: Case 1 Attack tree for Attack on Separator function & Sucker Rod Pump function

These portals provide detailed knowledge on how O&GP works, their components and functions, which can be targeted by an adversary. We have discussed these details throughout this research paper.

3. FUNCTION BASED APPROACH

The function-based approach [3] considers an important function of O&GP as a potential target function of attackers. By developing an understanding of the functions and components on which it depends, we narrow our focus to a single function at a time. Once we understand the dependencies, we build an attack tree to abstract the consequences of attacks. We demonstrate that an attack propagates from the cyber domain to the physical domain. We show the different data points corresponding to a function, which helps us to evaluate the resilience of the O&GP. We describe two cases in this section: Case 1: the targeted function is the oil/gas delivery from wellhead to the production plant and Case 2: the targeted function is the oil/gas delivery to end units after processing via pipelines.

3.1 Case 1: Cyber Attack on Oil/Gas Extraction from wellheads

In this use case, we evaluate the resilience of O&GP from the oil delivery point off view under the cyber attack. A sudden drop in the production of oil/natural gas at peak hours can cause loss of revenue, power generation and affect other systems like refineries and petroleum. As we know that the demand of natural gas is significantly high during winter months, it is possible that attackers launch attack when the demand is high with motive to have maximum impact on the system utility. The cyber-physical threat is based on the assumption that an attacker has gained access to a trusted utility system, which can also be thought of as insider threat [4], but it could be the result of subversion. The infrastructure responsible for extraction is sucker rod pumps, which are commonly used in the oil/gas industry. The attacker can compromise the PLCs by reprogramming them and affect the readings, which are given to pump controller that monitors its overall functionality. In order to discover how the cyber attack propagates to physical side of this system, it requires having better understanding of the system. We should know the factors on which the performance of the pump depends. The factors can be malicious or non-malicious. The malicious factors are the attacks performed by the attackers or disgruntled employee or insider threats [4] whereas non-malicious factors vary from situation to situation, including poor configuration policies, technology used for communication, or natural disaster. In the following section we describe the system under study and demonstrate how to create an attack tree corresponding to a function, which abstracts the cyber attack, which can harm that function.

The function under study is the delivery of crude oil to the refineries and production plants where products of oil/gas are manufactured. We ask at this stage how this function can be interrupted. In order to answer this question we identify the dependencies of the oil delivery in the system. The question arises - what are the components and functions that have a dependency connection with the oil delivery function. The main component in the oil delivery function is the delivery of raw oil from wellhead or seabed to the separator and separation of oil, gas and water so that oil can be fed to subsequent systems. If oil extraction fails, the production plant will stop for some time which will have cascading affects on the other systems like refineries, production plants and end customers. Mostly sucker rod pumps are used to extract the raw oil from well. The oil is fed to a separator since oil must have less than 1% (by volume) water and less than 5 lbm water/MMscf gas.

In this use case, we evaluate the resilience of the system by performing the sensitivity analysis on the oil delivery extraction and separation functions. Before that we need to understand how these functions work. The extraction function is performed by many sucker rod pump installed over the site of the O&GP. The performance of the system may be limited by power demands, maximum motor speed and thermal capacity, rod maximum load or rod fall velocity. PLCs are installed with every pumping system which send readings of each component of the pumping system and also receive commands from the administration in order to regulate its working. The speed commands can be sent from number of sources, which are keypad presets, potentiometer adjustments, serial data communications, and internal optimization controllers.

The separators [13] are a pressure vessel used for separating well fluids into gaseous and liquid components. As we have discussed that oil must have less than 1% (by volume) water and less than 5 lbm water/MMscf gas, the failure of this step affects the resilience of the system directly. If the components are not separated properly, the mixture is useless and oil/gas authorities will flare those gases. If the maximum amount of energy resource gets flared, the overall demand of oil and gas will be affected. There are number of factors which affect the performance of the separation function. These are operating pressure, liquid level control, temperature and other situational factors, which can arise in real time emergency.

Oil and gas separators can operate at range of high vacuum pressures ranging from 4,000 to 5,000 psi [13]. Psi stands for pounds per square inch. The separators maintain different level of pressures, which are: low pressure, medium pressure, or high pressure. The low-pressure separators operate at pressures ranging from 10 to 20 up to 180 to 225 psi. The medium-pressure separators operate at pressures ranging from 230 to 250 up to 600 to 700 psi. The high-pressure separators operate in the pressure range from 750 to 1,500 psi. If pressure reduces on a crude oil, tiny bubbles of gas are formed in side the oil. Because of this, foam is dispersed in the oil, which forms foaming oil. Foaming oil is a waste and reduces the capacity of the plant. The separator requires different controllers, which take readings from the separator system and send it to the centralized control system and takes commands from the same. In this research, we propose a framework to evaluate the resilience by drawing the line between

the acceptable and non-acceptable scenarios by varying the few variables (such as pressure in case of separator or motor speed in case of sucker rod pump.).

We have understood the functions and now we apply the function-based approach [3] on oil delivery functions. The main motive of this approach is to group all the attacks, which have same impact on the function. This approach also helps us to understand that how cyber failure propagates from cyber domain to physical domain. From our literature study, in case of power grids [3] sudden load drop (physical factor) that results from malicious remote disconnect (cyber-attack) is a physical factor that may lead to power delivery failure. In our case, reduction in pressure (physical factor) of the separator leads to foaming oil. This foaming reduces the capacity of oil/gas separators because longer time is required to separate a given quantity of foaming oil, which ultimately reduces the overall production of the oil/gas. We need to find the pressure limit under which pressure can be reduced so that plant keeps operating and producing oil/gas under attack. The change in pressure is physical change that has physical effects but controlled by the cyber factor.

The attack tree in figure 2 is divided into four levels. The first level of the attack tree represents the primary function failure (i.e. attacker's objective) that is oil/gas production failure. The second level represents the impact on the cyber (e.g. causing network traffic collisions) or physical system (e.g. causing drop in pressure in separator). The main factors are derived from this level. The third level represents the cyber-attack that stimulates the main factors. Different cyber-attacks may have the same impact on the system. By grouping those cyber-attacks under the same nodes, the evaluation process can be abstracted. The fourth level elaborates how the cyber-attack is implemented. Although we are interested in failures that result from malicious activities (cyber-attacks), the same failures may also result from non-malicious activities.

In figure 2, head end is compromised, which is responsible for monitoring the overall plant. There are number of ways in which the head end can be compromised, depending on the vulnerabilities in the system. We will not discuss the set of vulnerabilities of the system since it is out of the scope of this research. Once a head end is compromised, malicious commands can be sent by an attacker to the sucker rod pump, separators or other utilities to affect the resilience of the system. In this example, important factors that propagate from the cyber domain to the physical domain are: in a separator it is the amount of pressure reduced and the time over which it is reduced and in sucker rod pump: number of pumps compromised and the times over which they are remain compromised. The attack tree nodes in the second and third levels do not include all scenarios through which the top-level node can be harmed. For example, there might be unforeseen cyber-attacks that can cause sudden reduction in pressure or stoppage of pumps.

In addition, there might be faults from non-malicious events (for instance reduction in the power supplied to the plant which can cause a plant to stop for certain period of time) that have the same (and even worse) impact on the O&GPs. Such descriptions help us to concentrate on specific functions of the O&GP plant so that we can scope down data points to perform analysis specific to a particular function. In section 4, we describe various data points to evaluate the resilience of the system. For now, we discuss another scenario - distribution of oil/gas via pipeline systems.

3.2 Case 2: Pipeline Distribution for delivery of Oil/Gas to distant utilities

The pipeline system is responsible for transportation of oil/gas to distant utilities. The question arises that how such a huge network of pipelines are managed and monitored 24x7. Since one is not aware of un-predictable situations, how such network is controlled under rare or extreme events. For controlling such system we have SCADA systems. SCADA systems [1] have centralized control room, which monitor each activity relating to the transportation of energy. From transportation to maintenance of pipes, controlling oil/gas pressure, temperature, viscosity, flow control, compression, injection into the pipe etc. are controlled by SCADA systems. It has business rules, which compare the current situation with the expected situation and accordingly detects abnormality. Our focus is to understand the compression system and metering communication infrastructure.

Natural gas [9] [10] is pressurized as it travels through the pipeline. It is periodically compressed and pushed through pipelines. There are number of reasons because of which the speed of gas is slow and pressure is reduced. Some of them are large travelling distance, friction and geographic elevation. Because of these reasons compressor stations are placed in range of 40 to 70 miles apart along the pipeline. Even a small change in the property of the gas can cause damage to the pipeline and its surroundings (if gas is leaked). Referring to the Columbia Gas Transmission disaster [19] where Artemas Compressor Station caught fire when the internal surface of the pipeline got corroded. The failure resulted in a release of natural gas in the surroundings, which ignites fire. The failure was located on the pressurized side of the manual dump valve on Filter Separator-A. When system fails, the pressure in the filter separator was 1,940 psig, which was below the 2,400 psig Maximum Allowable Operating Pressure (MAOP). We will focus on the upper and lower limit of pressure in order to maintain the resilience of the system. But first we need to understand how compression works and why it is needed.

The compression station [9] consists of various components such as compressor units, electric power source, yard piping, safety systems and personnel working 24x7 in order to ensure the safe operation of the pipeline system. The compressor station handles the working of compressor units to re-pressurize the gas flowing through the pipeline. The pressure and temperature of natural gas increases when it is compressed. In order to protect the inner coating of the pipeline, the gas is cooled before it is returned to the pipeline. If the pressure of the gas is varied or not monitored, it can cause damage to the pipeline or the gas can leak as well. We will narrow down our focus towards the safe delivery of the energy to the end point utilities under cyber attack.

The function under study is the safe flow and delivery of processed oil/gas from production plants to end point utilities such as homes, manufacturing plants, petrol pumps etc. In the similar fashion, the question that we ask at this stage is: how can this function be interrupted? We must identify the dependencies of oil/gas delivery function in the system. So the next question is how these gases are delivered to end utilities. The main component in the oil delivery function is the delivery of produced oil/gas via pipelines systems. An attacker can target this function by changing the properties of the oil/gas flowing via pipeline and attacking the pipeline metering system via DDOS.

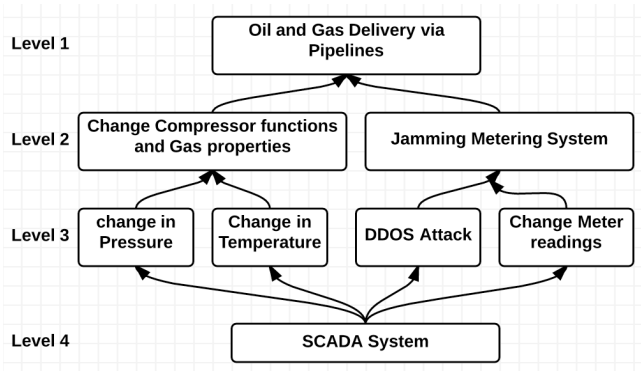


Figure 3: Case 2 Attack tree for Pipeline and metering system

In figure 3, we assume that attacker has control over the SCADA system and is in position to reprogram PLCs to change the gas pressure or temperature at the compressor stations. The attacker can also change readings coming from the sensors to the station due to which wrong picture is shown to the personnel working in control rooms. They are also in position to launch DDOS attack in order to disrupt the communication infrastructure. This will also affect the Cyber Security (CS) component of the pipeline system. The CS component protects the system from cyber attacks and provides integrity, availability and confidentiality services for the pipeline system. Disruption of these functions has direct consequences on the security of the pipeline system and impacts its overall resilience. This may cause legitimate packets belonging to higher-level functions (gas flow and delivery) to be dropped or delayed which impacts their performance and consequently their resilience. There are two cases: (1) what happens when pressure of the gas is monitored maliciously and (2) when communication infrastructure of the system is compromised. We need to evaluate the performance of the system in both the cases. In our future work, we will use performance metrics discussed in section 5, in order to evaluate the resilience of communication infrastructure. In this scenario, we not only have a radio mesh network but satellite communication, which takes readings from the sensors installed at various sites of the vast pipeline system. We have to include variables that will satisfy the proposed condition. After discussing these scenarios and attack trees, we describe the data points relevant to perform simulation and what simulation techniques are used to evaluate the resilience of the system.

4. DATA POINTS

It is imperative to figure out the data points, which will be useful in doing analysis and understanding how the system is working. In order to evaluate the resilience of the system, we need data corresponding to a targeted function (in our case it is oil/gas delivery from wellhead and via pipelines.). Table 1 and table 2 describe data points and types of data to be captured from them. We have chosen these data points because they describe the state of the overall system. The state of the oil/gas is determined by its physical properties such as temperature, pressure, speed etc. On another hand the state of the pipeline is determined by readings of valve readings, leakage detectors etc. In our experiments, we will try to change the state of the system by changing the properties of the oil and gas-using cyber-physical attacks simulation on our testbed. And then we can find the acceptable limits of the properties of the oil and gas up to which overall resilience of the system is not affected.

Table 1. Data points for Extraction & Separation and Pipeline

Extraction and Separation	Pipelining
Daily hours of operation	Pressure
Amount of oil extracted	Volume
Sucker rod pump: speed, pressure, temperature, count	Temperature
Daily requirement of electricity	Compressor readings at different levels
Properties of the gas flowing from sucker rod pump to separator	Leakage detector readings
Sensor readings at the separator	Valves readings
Reading from wellhead meters	Readings of physical properties

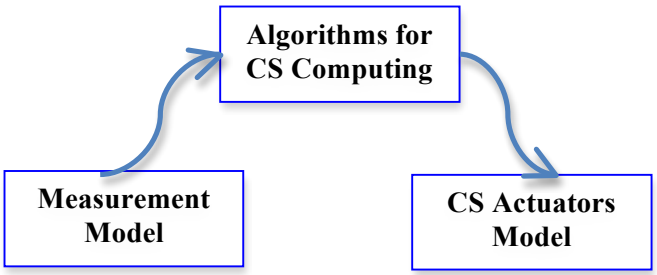
Table 2. Data points for IT Infrastructure

Information Technology Infrastructure
Type of Database maintained for storing business policies, logs etc.
Web application deployed and versions
Servers deployed and their versions
Firewalls deployed, their rules and logs
IDS/IPS
Operating systems and versions
Details of Past attacks and disasters
List of potential problems during normal course of operation
Types of PLCs and software implemented on them

We will not restrict our experiment to only changing the properties of the oil/gas but also we will simulate various cyber attacks on the network infrastructure of the system. It is possible that we will add, delete or modify variables on the basis of the function in our future research. These data points create situational awareness of the system and we can simulate the affects of the change in advance. Once we are able to collect this set of data, we can apply different modeling and simulation models to evaluate the resilience of the system by modifying various parameters.

5. MODELING AND SIMULATION

The research paper [7] inspires our model of Measurement-Algorithm-Control Modeling. Modeling is a procedure to represent a real world system in terms of hardware, software or both. Usually, a model of a system is represented by the mathematical relationships. It helps to simulate and analyze the real world system. Once a model is developed, simulation is performed to check whether system is responding appropriately to dedicated inputs. We use the Measurement-Algorithm-Control System based modeling to evaluate the resilience of O&GP. Figure 4 represents the modeling technique, which we use to evaluate the resilience of O&GP CPS. It has 3 main components: 1) Measurement Model, 2) Algorithms for Control system computing and 3) Control System (actuators). For our experiment, we will use RINSE [8] as a testbed. It provides realistic behavior of the system under cyber attacks.



Sensors for gathering: • Temperature • Pressure • Velocity of gas • Density of gas • Volume	Actuators • Valves • Temperature CS • Pressure CS • Speed of Sucker rod • Speed of gas
Meter readings	Isolate network which has been compromised
Compressor readings	Dynamic change in policies of the system
Number of stations working	Grant or Revoke access
Bandwidth of network	Stop or start of machines
Network Congestion for predicting DDOS attack	Reprogram PLCs

Figure 4. Measurement-Algorithm-CS Modeling approach

The measurement model represents the data collection model. Specific to a particular function, it describes various data points, which systems should measure so that we can perform complete analysis of the system. In our pipeline system for oil/gas delivery, the data points are discussed in Table 1. The table describes variety of variables, which we can use in different ways (separate or together by merging) to evaluate their effect on the O&GP CPS. The measurement model is the measurement of the variables from different sources and modifying those measurements according to our test bed.

The data from variety of sources are stored in a database (relational or other, we have not decided yet) so that we can replicate data and perform queries. Once the data sources are collected, we will design algorithms, which will take this data as input and perform analysis so that we can understand the dynamics of the system and evaluate its resilience. On the basis of the results of simulation, we can draw a line between the acceptable and non- acceptable limits of certain parameters. For instance, an attacker performs a DDOS attack on the communication infrastructure of the O&GP. There can be an expected delay in the packets reaching authorities and metering stations. By performing a DDOS attack, the attacker is able to compromise the availability of information in real time. Since critical infrastructure requires real time information for the control system to take action, it becomes difficult to confirm the state of system. Our algorithm will evaluate the dynamics of the communication infrastructure so that it can alert the control system personnel in case of detected attack. By calculating a metric (below) we can predict some non-acceptable changes to the system, which may happen in the near future. The variables, which we will evaluate to predict the unacceptable changes in the communication infrastructure, are:

- ✓ Maximum and available Network bandwidth at different intervals of time
- ✓ Mean time between failures [1]
- ✓ Packet delivery time (PDT) Round trip [3]
- ✓ Packet delivery ratio [3]
- ✓ Average End-to-End delay [3]
- ✓ Size of packets [3]
- ✓ Traffic rate [3]
- ✓ Network wired or wireless mesh
- ✓ Number of request with in and outside the network
- ✓ Number of attempts to perform DDOS attack
- ✓ Time window up to which system can tolerate no packet delivery at all.

Lastly, the computing system gives feedback to control systems on the basis of the results of simulations performed in the computing phase. This feedback concerns the changing properties of the gas flowing in the pipeline, sending commands to the compressor to start or stop working, sending commands to the sucker rod pump, opening or closing valves, isolating a server from the network incase of DDOS etc. This system is a closed loop system [7], we can evaluate the resilience of the system under cyber attack by modifying some inputs to the system and identify the boundary between acceptable and non-acceptable change. Now we describe how we conduct experiments once we have collected the data points from different sources.

We have planned to conduct experiments in terms of evaluating the resilience of the control systems, communication network and by modeling SCADA system using RINSE [8] and the Synergi Pipeline Simulator. Our objective is to develop a feedback loop that controls the state of the oil/gas in the pipeline system and via separators. The data that is collected defines the state of the gas (in Table 1) in the pipeline and state of the pipeline system. We will define the actions of the Algorithmic step by providing if-else rules for a particular scenario. We know the initial state and can perform various attacks as an adversary and see how the state of the system changes and what are the acceptable and unacceptable limits up to which system is resilient.

Using RINSE, we can simulate different network devices at different resolutions. These are network devices that control the state of oil and gas in the production plant, distribution pipelines and other utilities as described throughout the paper. We have planned to perform DDOS and Sybil attacks using the RINSE testbed to evaluate the state of the oil and gas in terms of its temperature, pressure, density, and velocity. We will design a radio mesh network of network devices that is a form of wireless ad hoc network. Wireless nodes overlay information from one node to another so that SCADA system receives and sends the control commands. Also, the sensors communicate with the control system on WIFI or NFC.

Once we have developed the prototype of the system, we can perform attacks as discussed above. In such attacks, we behave as an adversary and we change the configuration of the control system that changes the system's feedback and ultimately information about the correct state of the system is not delivered to the Control system. We will also implant our own botnets that will flood the network to prevent the delivery of the state of the system. In some experiments, we will change the properties of the gas to see what happens when an insider acts maliciously and how the system behaves in such scenarios.

Such experiments provide us the realistic network behavior when the devices are attacked and we can understand the dynamics of the system. The results of such experiments will be the acceptable limits of the properties of the oil and gas which should be maintained so that resilience of the system is not affected under

attack, number of working network devices so that correct information is delivered to the control system. This will help us to develop action plans to maintain the resilience of the system under such attacks in future. The main contribution of our research is when we know: what are those acceptable and unacceptable limits of the properties of the oil/gas, communication bandwidth and in terms of working nodes in the system when attack is happening and still the resilience of the system is maintained.

6. CONCLUSION

We have presented the function-based approach of evaluating the resilience of O&GP CPS under cyber attacks. The main motive of this approach is to group all the attacks, which have same impact on this system. This approach also helped us to understand that how cyber failure propagates to the physical failure of the system (by creating the attack tree). This is an ongoing research and we are in data collection phase.

We began our discussion with an overview of the workings of O&GP, its components, O&GP as cyber-physical system, types of attacks, and the workings of pipeline systems. We then proposed a function-based approach to evaluate the resilience of the O&GP. We identified the functions i.e. oil/gas delivery from wellhead to separator and via pipeline system and identified their dependencies in the system. Once dependencies were identified, we developed the attack trees corresponding to both the functions. The attack tree abstracts the types of attacks that affect a particular function, either maliciously or non-maliciously. Based on the understanding of the function and attacks possible, we described data points and a modeling approach we will use to evaluate the resilience of the system.

7. FUTURE RESEARCH

For now, we are acquiring data from utilities of O&GP, talking to experts in the field of oil and gas, deciding appropriate databases. In future, we have to develop a test bed to evaluate the resilience of the system. We will create our testbed on simulator such as RINSE, Synergi Pipeline Simulator, Network Simulator (NS) and EPANET for simulating different attacks on the system.

8. AKNOWLEDGMENTS

The work described in this paper was conducted under partial funding by Northrop Grumman Information Systems. The authors would like to thank Northrop Grumman group for their support and to Snigdha Goel, Mohit Gupta, and Disha Ajmani who participated in our research.

9. REFERENCES

[1] Kelvin T. Erickson, Ann Miller and E. Keith Stanek. Survey of SCADA System Technology and Reliability in the Offshore Oil and Gas Industry. *MMS TA&R Program Program SOL 1435-01-99-RP-3995*

[2] Vinay M Igure, Sean A Laughter, and Ronald D Williams. Security issues in SCADA networks. *Computers & Security, Elsevier 25(7):498–506. 2006.*

[3] Anas Al Majali . December. Function-based methodology for evaluating resilience in Smart Grid. Ph.D Dissertation, University of Southern California. 2014

[4] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry. Challenges for Securing Cyber Physical Systems. *Workshop on Future Directions in Cyber-physical Systems Security, DHS, 23, July, 2009.*

[5] Rinaldi, SMN. Modeling and Simulation critical Infrastructure and their interdependencies. *System Science, 2004. Proceedings of the 37th Annual Hawaii International Conference.*

[6] Clifford Neuman, Kymie Tan. Mediating Cyber and Physical Threat Propagation in Security Smart Grid Architectures. *Proceedings of 2nd International Conference on Smart Grid Communication (IEEE SmartGridComm) 2011.*

[7] Melin A, Kisner R, Fugate D, McIntyre T 2012. Minimum State Awareness for Resilient Control System under cyber attack. *Future of Instrumentation International Workshop 2012, 1-4.*

[8] D. M. Nicol, C. M. Davis and T. Overber 2009. A testbed for power system security evaluation, *International Journal of Information and Computer Security*, vol. 3, no. 2, pp. 114-131, October 2009.

[9] Description of Natural Gas Pipeline Technology Overview, Argonne National Laboratory Technical Report ANL/EVS/TM/08-5. http://corridoreis.anl.gov/documents/docs/technical/apt_61034_evs_tm_08_5.pdf

[10] Description of Natural gas. Wikipedia. https://en.wikipedia.org/wiki/Natural_gas

[11] US Environmental Protection Agency. http://www.epa.gov/cleanenergy/energy-and-you/affect/natural-gas.html

[12] US Department of Homeland Security, Energy Sector http://www.dhs.gov/energy-sector

[13] Separator https://en.wikipedia.org/wiki/Separator_(oil_production)

[14] US Department of Transportation, Pipeline and Hazardous Materials Safety Administration, Office of Pipeline Safety Eastern Region, Failure Investigation Report – Columbia Gas Transmission; Artemas Compressor Station Fire Failure Date 11/3/2011. http://www.phmsa.dot.gov/pv_obj_cache/pv_obj_id_8BC38156C05C00ED73D8A949D0D7FB8680FC2800/filename/CGT%20GT%20PA%202011-11-03%20508.pdf

[15] Norway's Oil Companies Largest Coordinated Attack. https://www.duosecurity.com/blog/norway-s-oil-companies-targets-of-largest-coordinated-attack

[16] Lloyd's Emergency risk report of 2015. http://darkmatters.norsecorp.com/2015/07/08/lloyds-losses-from-attack-on-power-grid-could-top-one-trillion-dollars/

[17] American Petroleum Institute: Energy Report of 2015. http://www.api.org/~/media/files/policy/soae-2015/api-2015-soae-report.pdf

[18] Brute Force Attacks on Internet-Facing Control systems. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf

[19] Columbia Gas Transmission Disaster http://www.ntsb.gov/investigations/AccidentReports/Pages/PAR1401.aspx