Modeling a Midstream Oil Terminal for Cyber Security Risk Evaluation

Rishabh Das, Thomas Morris

Chapter 9

MODELING A MIDSTREAM OIL TERMINAL FOR CYBER SECURITY RISK EVALUATION

Rishabh Das and Thomas Morris

Abstract High-fidelity cyber-physical testbeds that mimic the cyber and physical responses of real-world systems are required to investigate the vulnerabilities of industrial control systems. This chapter describes the construction of a large, virtual, high-fidelity testbed that models a midstream oil terminal. The testbed models interconnected tank farms, a tanker truck gantry, a shipping terminal and a 150 km pipeline connection to a refinery. The virtual midstream oil terminal helps experiment with cyber attacks, explore the impacts of cyber attacks in order to prototype and evaluate security controls, and support education and training efforts. The virtual midstream oil terminal is constructed using a novel modular modeling technique that segments the overall system into the physical system, cyber-physical link, distributed controllers, communications network and human-machine interface. Simulation results involving normal operations and cyber attack scenarios are presented. The midstream oil terminal testbed demonstrates that large-scale models of industrial control systems for cyber security research are feasible and valuable.

Keywords: Cyber-physical testbed, oil terminal operations, risk evaluation

1. Introduction

This chapter describes the architecture of a virtual midstream oil terminal testbed. The testbed incorporates five distinct subsystem models: (i) physical system; (ii) cyber-physical link; (iii) programmable logic controller (PLC); (iv) network; and (v) human-machine interface (HMI). The virtual midstream oil terminal is a high-fidelity model of a real midstream oil terminal. The components in the physical system model adhere to American Petroleum Institute (API) standards. The programmable logic controller model is a software ver-

sion of OpenPLC [2], which is available in hardware or software. The network model, which is provided by a VMWare workstation, supports the Ethernet, TCP/IP and Modbus/TCP protocols. The human-machine interface is the SCADABr open-source software product, which has been used to monitor and control real and virtual industrial control systems. The human-machine interface is the same software that is used in real midstream oil terminals.

The virtual midstream oil terminal testbed models three tank farms, a tanker truck gantry, a shipping terminal with two ocean-going oil tankers and a 150 km pipeline that is connected to a refinery. The three tank farms hold three liquid petroleum products: (i) gasoline; (ii) diesel; and (iii) aviation turbine fuel (ATF). The gasoline and diesel tank farms have four fixed/floating roof tanks each while the aviation turbine fuel tank farm has three dome roof tanks. Each tank farm includes a network of pipelines that supports recirculation, filling from external sources and transfers to the tanker truck gantry. Each tank farm also includes a set of pumps to move liquid cargo.

The tanker truck gantry incorporates three tanker truck models, each tanker truck with two internal tanks. The trucks must be grounded to initiate a fill operation.

The shipping terminal supports loading and unloading operations. Each ocean-going tanker has six internal tanks. The 150 km pipeline system includes a graduated pipeline that maintains pressure throughout the length of the pipeline.

In total, the physical system model incorporates 217 modeled sensors and actuators. Twelve networked programmable logic controllers are connected to the physical system model to implement distributed control. The programmable logic controllers communicate via Modbus/TCP over a TCP/IP network to the human-machine interface. The human-machine interface remotely polls the programmable logic controllers for system state information and provides supervisory control capability.

The high-fidelity testbed can be used to conduct cyber security research at a larger scale than most industrial control system testbeds available to researchers. Users can simulate cyber attacks and examine the impacts on physical system components. The scale of the virtual midstream oil terminal testbed enables researchers to model cyber attacks that exploit multiple components simultaneously or in sequence. This flexibility supports the reproduction of large-scale and cascading events, as well as analyses of the interdependencies existing between systems. Researchers can also use the pipeline testbed to prototype and evaluate the effectiveness of new cyber security controls.

Cyber security researchers often need data captured from industrial control systems during normal and cyber attack situations. Most industrial control system operators either do not have such data or will not share their data for reasons of sensitivity. The virtual midstream oil terminal can be used to produce the data required for research. Additionally, since the testbed is virtual, the testbed itself and the scripts used to generate interesting cyber attacks in the testbed are readily shared.

The virtual midstream oil terminal can be distributed electronically and can run on virtual machines in a cloud computing environment. This makes the testbed very useful for education and training. Students can use the virtual testbed to explore the functionality of industrial control systems, experiment with cyber attacks and evaluate security controls.

Modeling energy sector systems is highly relevant to cyber security research. Malfunctions of critical components such as oil terminals, pipelines, storage tanks and cargo vessels can cause fires, explosions or harm to the environment, which can impact energy supply and lead to large economic losses. In 2008, hackers successfully suppressed alarms and penetrated the communications network of the Baku-Tbilisi-Ceyhan pipeline [15]. The attack essentially blinded pipeline system operators. The pipeline was intentionally over-pressurized by the hackers, resulting in a rupture and explosion that spilled more than 30,000 barrels of crude oil. It took 24 hours to extinguish the resulting fire and the entire pipeline was not functional for eighteen days. This incident led to a serious political conflict between Georgia and Russia. In 2012, the Shamoon virus, released by the hacktivist group Cutting Sword of Justice, destroyed 30,000 computers at Saudi Aramco, which supplies 10% of the world's oil [11]. Saudi Aramco was forced to work offline for five months.

2. Related Work

Oil terminals and refineries are critical infrastructure assets that demand high operational vigilance. A malfunction, such as a pipeline rupture or vapor leak, can release a cloud that can ignite and cause a large fire or explosion. Zhou et al. [22] have performed an extensive study of 435 fire and explosion accidents in China. Sixty-six major fires and explosions occurred between 2000 and 2013, causing a total of 390 deaths and 950 injuries. The study also reveals that 76.09% of the accidents were caused by vapor clouds from fuel leaks, pipeline ruptures and mechanical failures.

Several power system testbeds have been developed for simulating cyber attacks against power systems [12]. The Testbed for Analyzing Security of SCADA Control Systems (TASSCS) has been developed to evaluate the effects of eight types of cyber attacks [16]. It provides a high-fidelity simulation of a SCADA network that uses the Modbus and DNP3 protocols. TASSCS does not simulate programmable logic controllers; instead, a Modbus server is hosted on a control server. As a result, vulnerabilities associated with programmable logic controllers cannot be examined using TASSCS.

Adhikari et al. [1] have developed a testbed specifically for cyber security research related to bulk electricity transmission systems. The testbed implements wide-area measurement functionality using a real-time digital simulator, hardware-in-the-loop protection relays, phasor measurement units and phasor data concentrators. However, the testbed does not incorporate any programmable logic controllers.

Morris et al. [18] have developed a high-fidelity gas pipeline testbed for collecting data for intrusion detection research. The testbed is modular and

portable, but Python programs are used for control instead of employing simulations of actual programmable logic controllers.

DeterLab is a power system testbed used by more than 2,600 researchers [17]. It incorporates 400 general purpose computing nodes and supports simulations of cyber attacks such as SQL injection, TCP SYN flooding and worms. DeterLab enables high-fidelity simulations, but its architecture is not modular. The security of a power system can be analyzed as a whole; however, researchers interested in analyzing specific industrial control system problems such as programmable logic controller functionality, SCADA network communications and physical system vulnerabilities cannot use this testbed. Additionally, the computing power required to operate the testbed significantly reduces its portability.

At this time, no published research exists related to midstream oil terminal testbeds. Therefore, the virtual high-fidelity testbed that models a midstream oil terminal should be of considerable interest to researchers. The testbed simulates real-world programmable logic controllers and is also lightweight and portable.

3. Testbed Architecture

This section describes the architecture of the virtual midstream oil terminal testbed.

3.1 Virtual Testbed Modular Framework

The midstream oil terminal testbed is implemented using a modular framework that is capable of modeling any SCADA system. The framework organizes a SCADA system in terms of five major components: (i) physical system; (ii) cyber-physical link; (iii) digital control system; (iv) communications network; and (v) human-machine interface. Each of the five major components is replaced by a virtual counterpart.

Figure 1 shows how each modularized component of a SCADA system is replaced by its equivalent virtual counterpart. The modular architecture described in this section and used to implement the midstream oil terminal testbed was also employed by Alves et al. [3] to model a laboratory-scale gas pipeline. Alves and colleagues compared a physical gas pipeline against a virtual model of the same pipeline. They demonstrated that the virtual testbed provided high simulation accuracy for normal operations as well as for cyber attack scenarios.

The physical system is an operational system such as an oil terminal, power system, chemical plant or manufacturing plant. In the virtual model, the physics and operational dynamics of the physical system are simulated via Simulink, a graphical programming environment for simulating, analyzing and modeling multi-domain dynamic systems. Simulink provides toolkits that model a variety of physical system components. The physical system model also includes sensors and actuators. Sensors are modeled in Simulink by connecting internal signals to probes. Actuators are modeled by connecting binary inputs

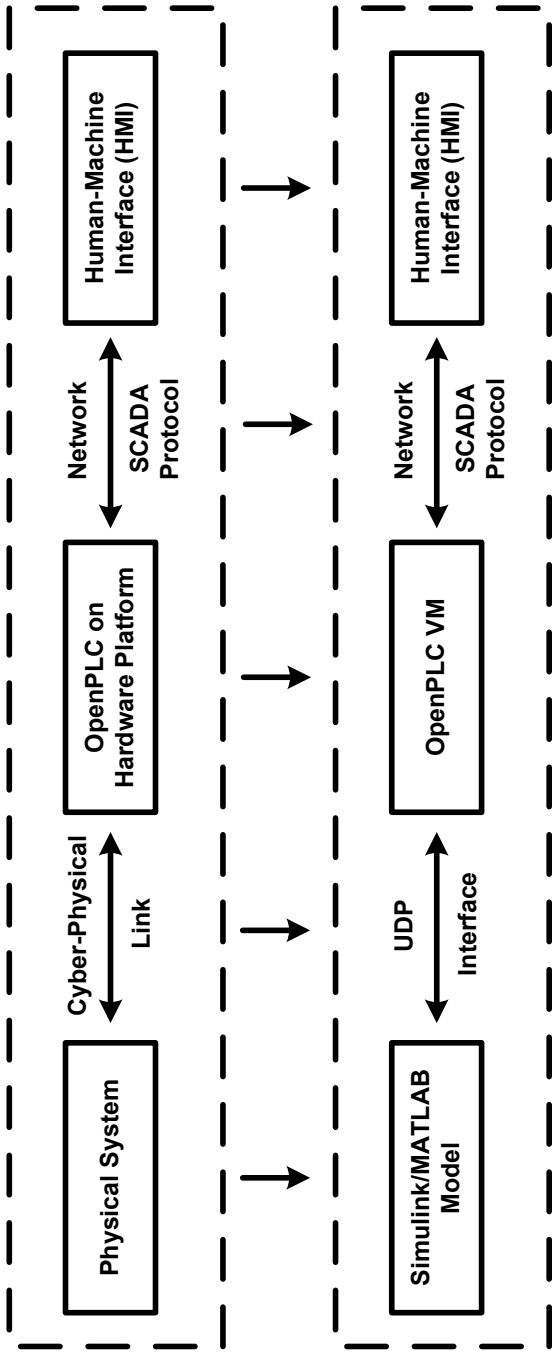

Figure 1. SCADA components and their virtual counterparts.

from the cyber-physical link to control physical components such as valves and switches. The physical system may be modeled using tools other than Simulink when appropriate.

Sensors and actuators are connected to the programmable logic controller via cyber-physical links. A cyber-physical link is as simple as a wire or it may use sensor network communications technologies such as WirelessHart and Zigbee [21]. When modeling wires, the physical connectivity between sensors and actuators and a programmable logic controller is virtualized using UDP sockets. In a real system, each sensor and actuator is independently connected by wires to a programmable logic controller. Likewise, in the virtual model, each sensor and actuator communicates with a programmable logic controller using a unique UDP port. The unique UDP ports enable the programmable logic controller to maintain separate communications with each sensor and actuator, thereby maintaining fidelity with the physical system.

A programmable logic controller is a computing device that monitors and controls the physical process and provides a network link for supervisory monitoring and control at a control center. It connects to sensors and actuators via cyber-physical links. The virtual testbed models programmable logic controllers using OpenPLC [2]. OpenPLC is open-source programmable logic controller software that supports all five IEC 61131-3 standard programming languages and the Modbus/TCP and DNP3 protocols. OpenPLC supports a wide variety of hardware platforms. In the case of a virtual testbed, software versions are executed in virtual machines using Windows or Linux operating systems.

The human-machine interface is a dedicated graphical user interface used by operators to remotely monitor and supervise an industrial process. The human-machine interface communicates with programmable logic controllers using standard communications protocols and provides the operator with the real-time status of the physical system. The human-machine interface may run on a virtual machine or on a separate host computer. Communications between a programmable logic controller and human-machine interface can employ virtual networking provided by a hypervisor or a real network. The human-machine interface software and application-specific user interface for the process control system are typically the same for real-world and virtual versions.

3.2 Midstream Oil Terminal Testbed

The midstream oil terminal testbed was implemented using the modular framework described above. The physical system was modeled using the Simulink SimHydraulics toolkit, which provides constructs for modeling pipes, bends, valves and other hydraulic components. The exact configurations of the various physical system sub-components are described later in this chapter.

The physical system model incorporates 217 sensors and actuators. The sensors and actuators are connected to twelve virtual programmable logic controllers using a virtual wire bridge with a UDP socket for each sensor and actuator. Each virtual programmable logic controller is an OpenPLC instance

Table 1. Components controlled by the programmable logic controllers.

PLC	Controlled Component
1	Marine tanker pipeline loading
2	Marine tanker pipeline unloading
3	Pipeline transfer operation
4	Oil tanker discharging
5	Marine tanker loading
6	Tanker truck gantry
7	Gasoline pump house
8	Diesel pump house
9	Aviation turbine fuel pump house pipeline
10	Gasoline tank farm
11	Diesel tank farm pipeline
12	Aviation turbine tank farm pipeline

that runs on a Debian virtual machine. The programmable logic controller programmation was developed using ladder logic. The actuators and sensors in the Simulink model of the virtual oil terminal communicate with the programmable logic controllers using a software interface hosted by the PLC 1 virtual machine. The software interface distributes the sensor readings to the programmable logic controllers and delivers control commands and information from the programmable logic controllers to the Simulink model.

The midstream oil terminal human-machine interface was created using SCADABr, an open-source, web-based, human-machine interface development environment. The Modbus/TCP protocol is used for communications between the human-machine interface and programmable logic controllers. The attack scenarios simulated in this research assume that the attacker is physically connected to the network that houses the programmable logic controllers. Since programmable logic controllers enable clients to connect to them without authentication, an attacker can connect to any programmable logic controller and query the status of the registers and coils.

Figure 2 presents a high-level layout of the simulated testbed. Table 1 lists each of the twelve programmable logic controllers and the component it controls.

4. Standards and Components

Oil and gas sector operations are divided into three sectors: (i) upstream; (ii) midstream; and (iii) downstream. The upstream sector generally involves exploration and drilling to locate and recover crude oil and natural gas. The midstream sector moves the materials from remote production locations to population centers. The downstream sector refines the materials into petroleum

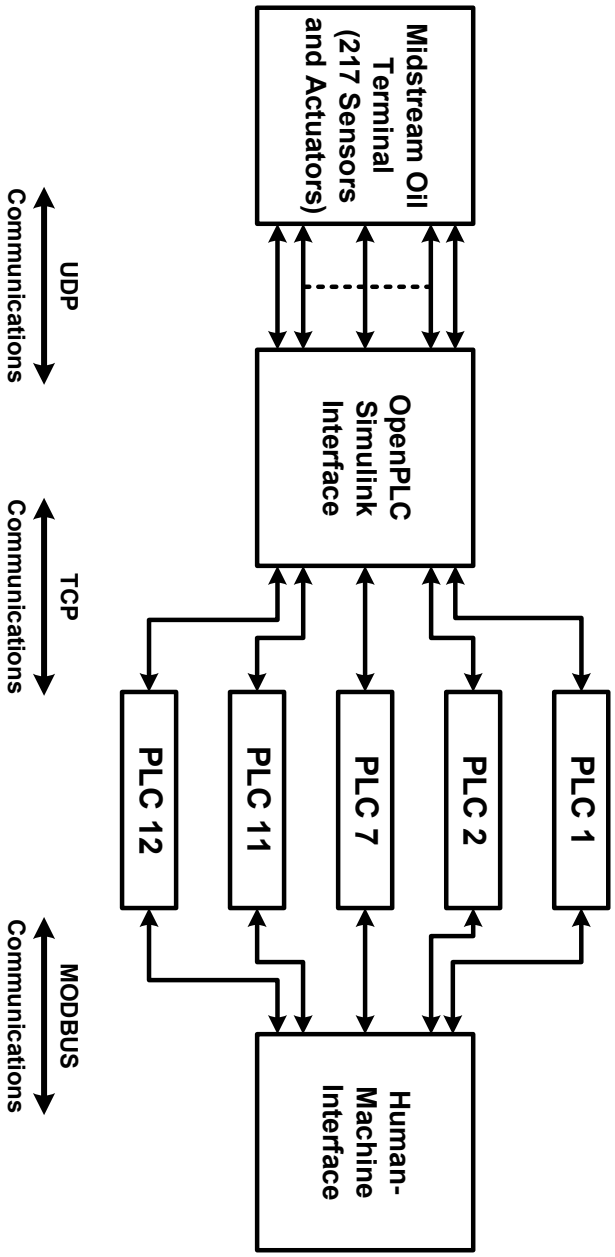

Figure 2. Simulated testbed.

Table 2. Midstream oil terminal component specifications.

Standard	Description
API SPEC 5L [6]	Pipeline specifications (tank farm)
API SPEC 6D [8]	Pipeline valve specifications
API SPEC 6H [5]	Pipeline connector specifications
API SPEC 11L6 [4]	Motor and pump specifications
API SPEC 12B [7]	Liquid cargo tank specifications
API RP 1007 [9]	Tanker truck specifications
API RP 1109 [10]	Pipeline transfer operation specifications

products and distributes the products to the retail market. Tanker trucks, marine tankers, pipelines and storage terminals are employed in all three sectors.

Figure 3 shows an overview of the virtual midstream oil terminal. The midstream oil terminal stores gasoline, diesel and aviation turbine fuel (ATF). Each of the three tank farms has a pump house. The tank farms are connected to a tanker truck gantry, which loads fuel into tanker trucks. The tank farms also load and unload marine tankers (MTs). The tank farms are connected to the marine tankers via a 12 km pipeline. The tank farms are also connected to a shore refinery via a 150 km cross-country pipeline. The network of pipelines and valves is abstracted in Figure 3.

4.1 Midstream Oil Terminal Standards

The American Petroleum Institute (API) promulgates standards for oil terminal equipment and components. The relevant American Petroleum Institute standards were followed to achieve high fidelity between the simulated model and a real midstream oil terminal. Table 2 lists the standards used in the simulation. The specifications and operational guidelines for marine tanker operation documented in the International Safety Guide for Oil Tanker and Terminals (ISGOTT) [14] were also used in the simulation.

4.2 Midstream Oil Terminal Components

This section provides detailed descriptions of the major components and activities of the midstream oil terminal: (i) tank farms; (ii) pump houses; (iii) tanker truck gantry; (iv) pipeline transfer; and (v) vessel operation.

Tank Farms. A tank farm is a network of tanks, valves, pumps and pipes that stores cargo in an oil terminal. The tank farms form the core of a midstream oil terminal because all terminal operations are either from or to tank farms. The presence of a fuel-air mixture makes a tank farm susceptible to fire and explosion due to the storage of volatile cargoes such as diesel, gasoline and aviation turbine fuel. According to a case study performed by Zhou et al. [22],

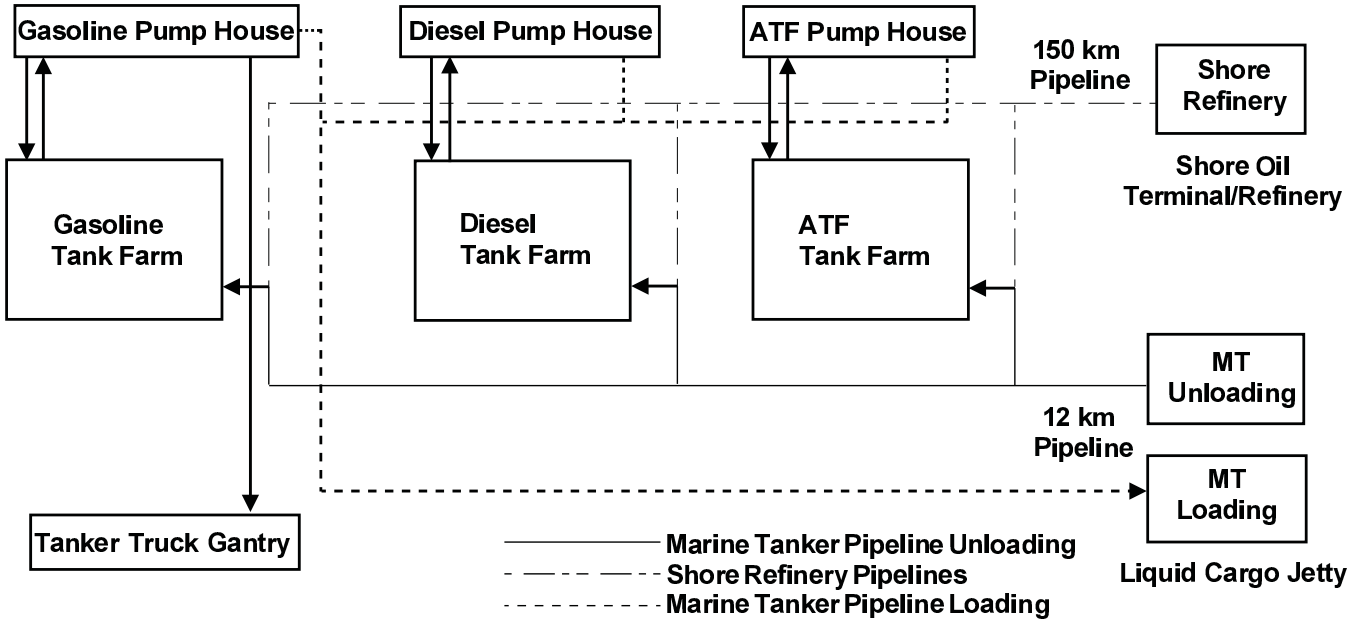

Figure 3. Midstream oil terminal subsystems with pipeline connections.

Table 3. Tank farm specifications.

	Gasoline Tank Farm	**Diesel Tank Farm**	**ATF Tank Farm**
Number of Tanks	4	4	3
Type	Fixed/floating roof	Fixed/floating roof	Dome roof
Height	15 m	15 m	18 m
Diameter	20 m	20 m	18 m
Inlet	16 in	16 in	18 in
Outlet	18 in	18 in	20 in
Inlet/Outlet	16 in	16 in	16 in

76.09% of major accidents in oil terminals were due to the presence of a fuel-air mixture and 25.75% of major accidents originated in tank farms. Due to the critical nature of a tank farm, a number of standards are adopted to ensure safe operation. API SPEC 5L [6] and API SPEC 12B [7] specify tank farm pipeline and valve configurations, respectively.

The modeled midstream oil terminal has three tank farms, one each for gasoline, diesel and aviation turbine fuel. Volatile cargoes such as diesel and gasoline are susceptible to vapor loss [19]. API SPEC 12B [7] requires the use of fixed roof or floating roof tanks for storing these cargoes. Aviation turbine fuel is a type of superior kerosene oil with quality standards that require less than 15 ppm of water to be present in stored or dispatched fuel [20]. To adhere to these requirements, fixed and floating roof tanks cannot be used; instead, dome roof tanks with fixed ceilings are employed for storage.

Table 3 lists the numbers of tanks, tank types, tank heights, tank diameters, inlet diameters, outlet diameters and inlet/outlet diameters for the tank farms modeled in Matlab Simulink for the virtual midstream oil terminal. There are three tank farms in the model, one each for gasoline, diesel and aviation turbine fuel. The gasoline and diesel tank farms have four tanks each while the aviation turbine fuel tank farm has three tanks. The tanks are named according to ISGOTT naming conventions [14]. Each tank is named TK followed by the tank farm number and tank number. For example, the first tank in the diesel tank farm is TK 21 and the second tank in the aviation turbine fuel tank farm is TK 32.

Each tank has three dedicated pipeline connections: (i) receipt; (ii) dispatch; and (iii) recirculation. The receipt pipeline receives cargo from a marine tanker or from the shore terminal via a pipeline transfer. The dispatch pipeline connection is used as an outlet; this pipeline transfers cargo out from the tank to a tanker truck, marine tanker or another tank. The recirculation pipeline connection is used for operations within the tank farm. Operations such as inter-tank transfers using gravity or pumps are performed using the recirculation connection. The recirculation connection can be used as a tank inlet or outlet.

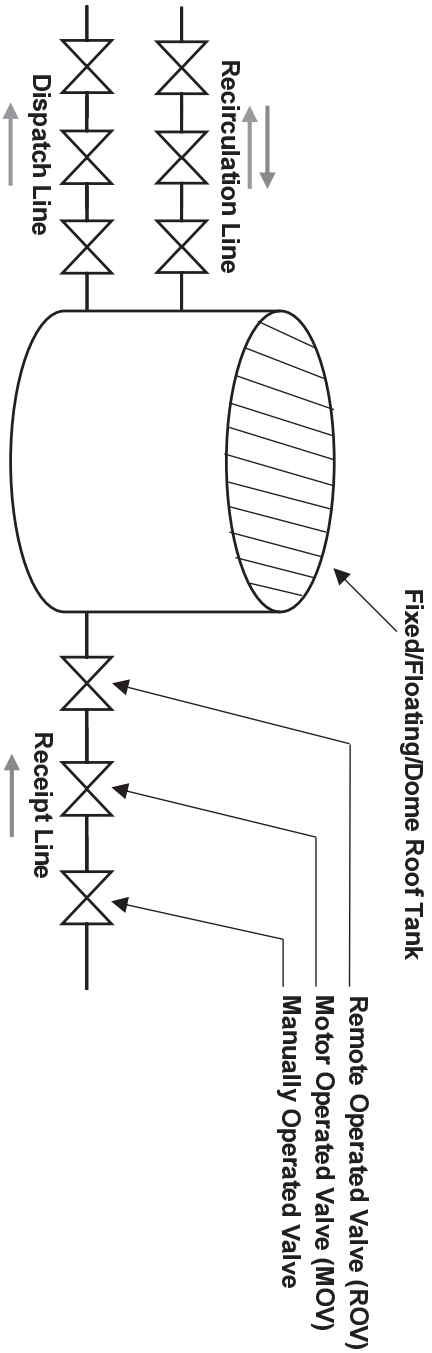

Figure 4. Typical simulated tank.

Table 4. Pump house specifications.

	Gasoline Pump House	**Diesel Pump House**	**ATF Pump House**
Pump Specifications	Centrifugal $1 \times 100\,m^3/h$ $2 \times 200\,m^3/h$ $2 \times 500\,m^3/h$	Centrifugal $1 \times 100\,m^3/h$ $3 \times 250\,m^3/h$ $1 \times 500\,m^3/h$	Centrifugal $3 \times 250\,m^3/h$
Inlet	16 in	16 in	18 in
Outlet	20 in	20 in	24 in
Drive Motor Specifications	Induction 1×40 kW (79 A) 2×90 kW (180 A) 2×200 kW (345 A)	Induction 1×40 kW (79 A) 3×110 kW (192 A) 1×200 kW (345 A)	Induction 3×110 kW (192 A)

According to the Oil Industry Safety Directorate (OISD) Standards 169, 118 and 129 and the recommendation by Lal et al. [13], three types of valves, each controlled by a different actuation mechanism, should be used between each tank and its pipeline connection. Hence, in the virtual midstream oil terminal model, each pipeline connection to a tank incorporates three valves. The valve closest to the tank is controlled pneumatically, the second valve is electrically actuated using a motor and the third valve is operated manually. Figure 4 shows a typical modeled tank with three pipeline connections and valves. The pneumatic valve, labeled remote operated valve (ROV), and the motor operated valve (MOV) can be operated remotely from the human-machine interface. The manual valve is operated physically. In the Matlab Simulink model, manual valves are operated by toggling a switch manually.

Pump House. The pump house is the heart of the midstream oil terminal. Each tank farm has a dedicated pump house. The gasoline, diesel and aviation turbine fuel pump houses have five, five and three pumps respectively. The modeled pumps are of various sizes and can be connected in parallel to achieve the desired flow rate. The valves in the pump houses can be remotely configured to dispatch cargo from tanks to marine tankers, tanker trucks or to other tanks in the tank farm. The gasoline and diesel pump houses have dedicated pipelines for transferring cargo to the tanker truck gantry. Per API SPEC 11L6 [4], the pumps use three-phase induction motors that deliver constant torque via a universal coupling connected through a common shaft to the centrifugal pumps. Table 4 shows the detailed specifications for the pumps in the virtual midstream oil terminal.

Tanker Truck Gantry. The tank truck gantry is the most operationally active area of the terminal. The presence of moving trucks and open volatile

Table 5. Tanker truck loading bay specifications.

	Bay 1	**Bay 2**	**Bay 3**
Cargo	Gasoline	Diesel	Gasoline and Diesel
Loading Arm	2 × 6	2 × 6	1 × 6 1 × 6
Bay	Single cargo express loading bay	Single cargo express loading bay	Mixed cargo loading bay
Valve	Butterfly valve for flow regulation		
Tanker Trucks	2 × 6 kl tankers Safety features include overfill sensors, tanker truck ground connections, flow regulators for loading arms		

cargoes makes this area susceptible to fires and explosions. More than 51% of major accidents in oil terminals originate in tanker truck gantries [22].

A tanker truck gantry typically has several loading zones with dedicated loading arms for transferring liquid cargoes into tanker trucks. The allowable cargo capacity in a tanker truck is between 2,000 and 16,000 gallons (7,570 and 49,205 liters). At least 3% of a tank must be left empty to provide space for product expansion.

A tanker truck gantry with three loading bays is modeled in the virtual midstream oil terminal. One bay is allocated for gasoline, the second bay is for diesel and the third mixed bay can load gasoline or diesel. Aviation turbine fuel cannot be loaded on a truck.

Each modeled tanker truck has two internal 6 kl tanks. API RP 1007 [9] states that the body of a tanker truck must be electrically grounded during loading operations to prevent static charge accumulation in the tanker truck. Therefore, each modeled tanker truck bay has sensors connected to a programmable logic controller that detects if the tanker truck is not grounded correctly. The programmable logic controller prevents the loading operation if the truck is not electrically grounded. The tanker truck gantry programmable logic controller also regulates product flow using a butterfly valve. An overfill sensor connected to the programmable logic controller stops product flow when the tank truck is full. Table 5 provides the specifications of the three modeled loading bays.

Cross-Country Pipeline. The virtual midstream oil terminal testbed models a 150 km underground cross-country pipeline from a shore-based oil refinery to the tank farm. Pipeline transfer is a cost efficient and safe way to transfer liquid cargo over long distances. Operational hazards are minimized because the volatile cargo is never exposed to the ambient environment. Due to the length of a pipeline, remotely-monitored sensors provide pipeline state in-

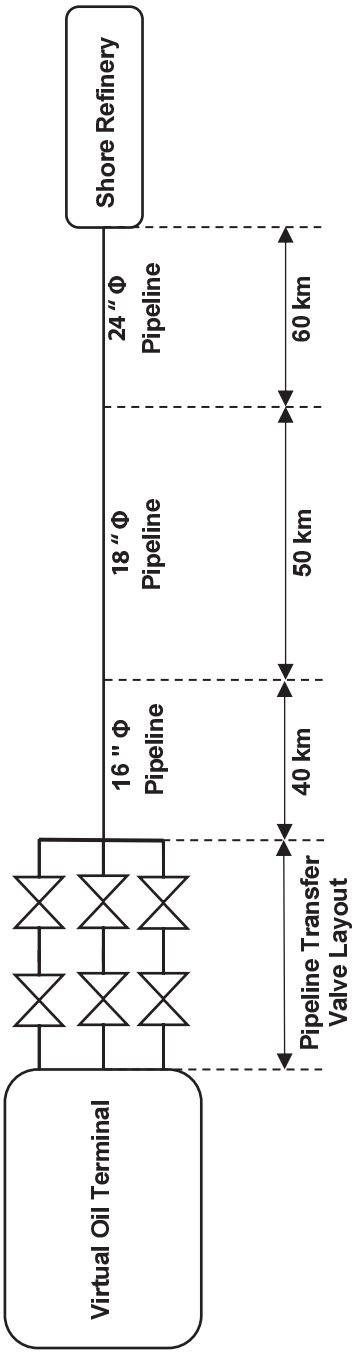

Figure 5. Cross-country pipeline.

formation to operators. A cyber attack that spoofs pipeline sensor readings can disrupt and harm the pipeline transfer operation [15]. The modeled pipeline complies with API RP 1109 [10]. Multiple flow rate and pressure sensors are modeled to enable remote monitoring of the status of the pipeline transfer operation. The diameter of the pipeline decreases farther from the source to compensate for the drop in pressure due to the long-distance pumping operation. Figure 5 shows the layout of the cross-country pipeline.

Terminal-to-Jetty Pipelines. A wide array of liquid and liquefied gas cargoes are transferred across large distances using marine tankers. Marine tanker loading and unloading require the use of many cyber-physical systems, including a marine loading arm (MLA), on shore holding tanks, pumps, on-ship tanks on-ship pipelines.

The testbed simulates two terminal-to-jetty 12 km pipelines. One pipeline is dedicated to vessel loading and the other to vessel unloading. ISGOTT [14] has published safety regulations for oil tanker cargo operations. During cargo operation, double-wall segregation of valves is mandatory, i.e., two valves must separate the operating pipeline from other pipelines. As a result, the modeled terminal-to-jetty pipeline has six valves, two for each cargo type on the terminal side as shown in Figure 6.

The terminal-to-jetty pipelines are coupled to the manifolds of marine tankers using marine loading arms. A marine loading arm is a sophisticated pipeline that connect the shore pipeline to a marine tanker to facilitate cargo transfer. A marine loading arm incorporates safety features that prevent oil spillage and offer a mechanism for the connection and disconnection of the shore pipeline and marine tanker. Position sensors are used in a marine loading arm to sense the orientation of the marine tanker. If the ship drifts away from the jetty, an emergency valve called a power emergency release coupling is actuated to release the marine loading arm from the ship and close the pipeline valves to prevent spillage. This emergency release mechanism is crucial to the dynamic jetty-vessel coupling system because it prevents damage to the loading arm.

Each simulated ship has six tanks; three port-side tanks (P1, P2, P3) and three starboard-side tanks (S1, S2, S3). The internal pipeline connections are not modeled and the simulation does not consider the effects of ballast tanks and ballasting operations that pump sea water into and out of a ship to compensate for the outgoing and incoming liquid cargo.

5. Simulation Results

The midstream oil terminal can simulate a variety of normal cargo operations. The supported normal cargo operations include inter-tank, tank-to-tanker-truck, tank-to-ship, ship-to-tank and refinery-to-tank transfers. In addition to normal cargo operation simulations, cyber attacks can be launched against the cyber systems modeled in the midstream oil terminal. This section describes the simulation results obtained for inter-tank transfers using gravity and using pumps under normal and attack scenarios. Other normal and attack

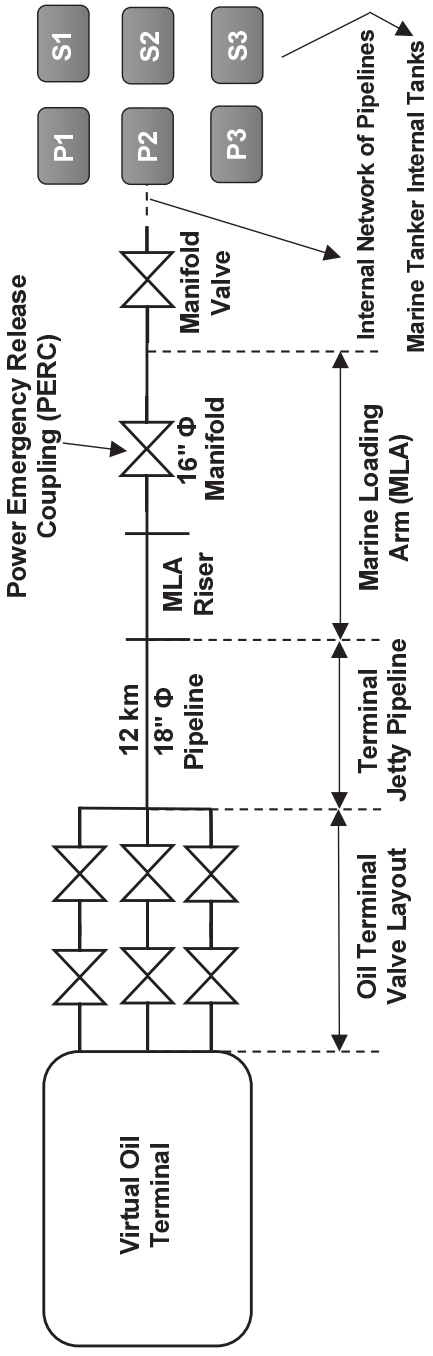

Figure 6. Marine loading operation.

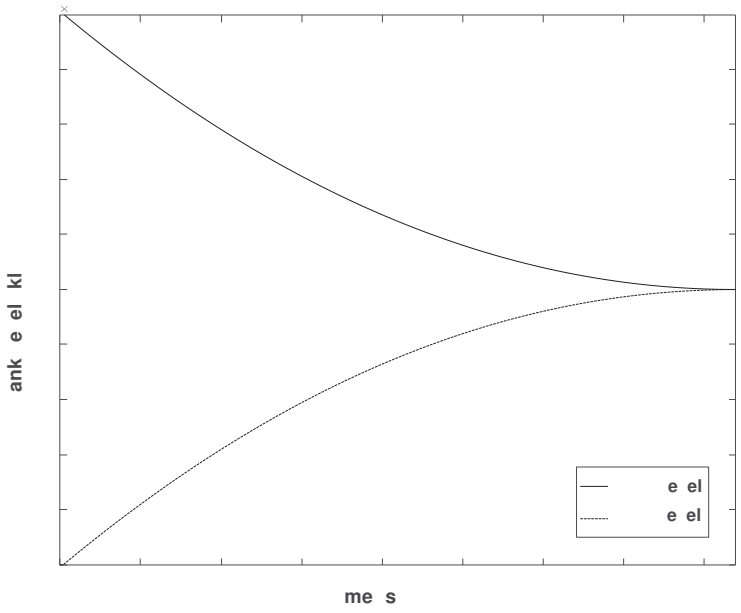

Figure 7. Inter-tank transfer operation using gravity.

scenarios have been simulated and validated using the testbed, but they are not described here for reasons of brevity.

5.1 Inter-Tank Transfer Using Gravity

Inter-tank transfer moves liquid cargo from one tank to another one in a tank farm.

An inter-tank operation may leverage gravity (head) associated with the difference in the liquid levels in the two tanks. For an inter-tank transfer using gravity, the valves between the two tanks are opened to enable cargo to flow from the tank with the higher liquid level to the tank with the lower liquid level. Over time, the tanks reach equilibrium, at which point both the tanks have the same liquid level.

Figure 7 shows the liquid levels in gasoline tanks TK 11 and TK 12 observed from the human-machine interface during an inter-tank transfer operation. Three valves (remote operated, motor operated and manual) in the recirculation pipeline of each tank are involved in the inter-tank transfer. All three valves are opened to initiate transfer and may be closed at any time during the transfer. Figure 7 shows that the flow rate between tanks is not constant. In fact, the flow rate is dependent on the difference between the liquid cargo levels in the tanks – the greater the difference in levels, the greater the flow rate.

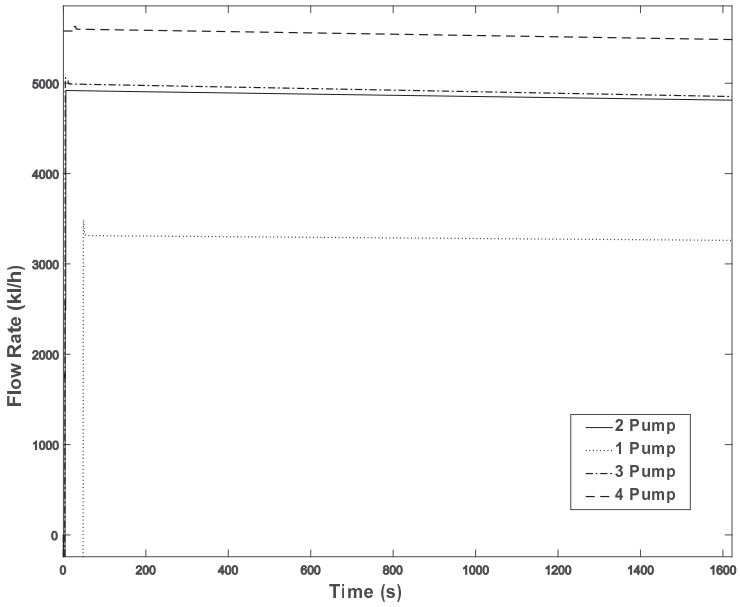

Figure 8. Inter-tank transfer operation using centrifugal pumps in parallel.

5.2 Inter-Tank Transfer Using Pumps

In some cases, the difference in liquid levels in the two tanks (head) may not be adequate to facilitate the transfer of cargo with a sufficient flow rate, or the transfer of cargo may have to go against gravity. In these cases, an inter-tank transfer is accomplished using pumps. To facilitate the operation, the human-machine interface is used to connect the dispatch pipeline of the source tank to the inlets of the relevant pumps and the pump outlets are connected to the recirculation connections of the destination tanks. The human-machine interface is used to start and stop the pumps at the beginning and end of the operation, respectively.

Figure 8 shows sensor readings from the inlet flow rate sensor at the destination tank during inter-tank transfer operations. The inter-tank transfer was repeated four times with one, two, three and four pumps working in parallel to complete the transfers. The graphs are labeled with the numbers of pumps used for the operations. When a single pump is used, a delay of 20 to 30 seconds occurs between the start of the transfer operation and the increase in the flow rate observed at the tank inlet. The delay is primarily because the air inside the pipeline must be pushed out before the cargo can flow. When multiple pumps are used, the air is pushed out much faster, causing the flow rate to increase at a faster rate, which appears to be instantaneous in Figure 8. As the number of pumps used increases, a higher flow rate is seen due to the accumulation of flow from more pumps in parallel. The three-pump case has a

slightly higher flow rate than the two-pump case because the third pump has a low rating of $100\,m^3/h$.

5.3 Cyber Attack Scenarios

The midstream oil terminal testbed can be used to simulate network-borne attacks that target programmable logic controllers or the human-machine interface, physical attacks against process components, attacks that alter the programmable logic controller programmation or firmware, attacks that alter the human-machine interface programmation and other attacks on the human-machine interface executables (e.g., buffer overflows and database injection attacks). During a simulated attack, all the testbed components continue to simulate the system, enabling the behavior of the system to be observed and analyzed. This section describes man-in-the-middle (MiTM) and denial-of-service (DoS) attacks during a tanker truck loading operation. Also, it discusses an injection attack against a tank valve during a tanker truck loading operation.

Man-in-the-Middle and Denial-of-Service Attacks. This section presents the simulation results for two cyber attack scenarios. The first is a man-in-the-middle attack during a tanker truck loading operation, which alters sensor data in transit between the programmable logic controller and human-machine interface. This causes the human-machine interface to present incorrect sensor data to the operator. The second attack is a volumetric denial-of-service attack on the human-machine interface. This attack causes the human-machine interface to stop polling the programmable logic controller for system state updates. The actual process state and the state presented by the human-machine interface are plotted for the two attacks. These scenarios highlight the ability of the virtual midstream oil terminal testbed to model network-borne cyber attacks and the ability to observe the actual physical system state and the state as seen by the human-machine interface.

Figure 9 shows the flow rates measured by a sensor in the tanker truck gantry during a tanker truck loading operation. One curve shows the flow rate observed at the human-machine interface and the other shows the actual flow rate. The majority of Figure 9 shows the normal tanker truck loading operation. However, the effects of the two cyber attacks are also observed.

The first attack occurred between 100 and 270 seconds. During this time period, the man-in-the-middle attack compromised the link between the human-machine interface and programmable logic controller, and altered the flow rate measurements transmitted from the programmable logic controller to human-machine interface. Ettercap was used to perform the ARP spoofing attack.

A man-in-the-middle attack is especially dangerous for a pipeline. In the Baku-Tbilisi-Ceyhan pipeline incident [15], attackers suppressed alarms, altered system control in order to affect the process state and blinded operators who were monitoring the pipeline. The man-in-the-middle attack can be used to inject, alter or drop network traffic between the human-machine interface and programmable logic controller in both directions. Injecting control packets

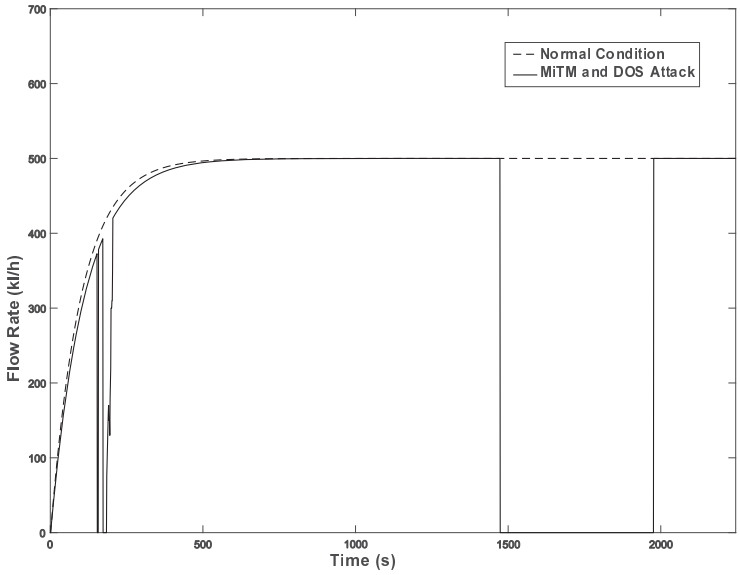

Figure 9. Tanker truck loading flow rates during normal and attack conditions.

can change the process state; altering and/or dropping sensor data can blind operators and upstream controllers. Figure 9 shows that, between 100 and 270 seconds, the flow rate sensor data was altered to show large (spurious) fluctuations in the flow rate. Such an attack could induce the operator to initiate a supervisory control action based on the false sensor data and ultimately move the physical process into an unsafe state.

The second attack involving volumetric denial-of-service occurred between 1,470 and 1,950 seconds. During this time period, the attack targeted the human-machine interface. The open-source Hping3 software was used to perform the attack. Figure 9 shows that from 1,470 to 1,950 seconds, a flow rate of 0 kl/h was presented by the human-machine interface while the actual flow rate remained at 500 kl/h. During the attack, the human-machine interface was overwhelmed and was unable to query the programmable logic controller in order to obtain the current state of the process. This attack prevented the operator from receiving the true state of the system.

Injection Attack. Liquid cargo operations in an oil terminal often involve multiple subsystems. For example, the tanker truck loading operation involves the tank farm, pump house and tanker truck gantry. The liquid cargo stored in a tank farm is transferred into the internal tanks of the tanker trucks using the centrifugal pumps in the pump house. The state reflected by the simulation at any given instant during the cargo operation considers the states of all the interconnected subsystems (tank farm, pump house and tanker truck gantry,

vessel operation and pipeline transfer) in the oil terminal. Therefore, during a tanker truck loading operation, if an attacker manages to sabotage any of the oil terminal components, the effects of the attack may be evident across multiple interdependent subsystems. This section discusses the impact of an injection attack on a tanker truck loading operation when the dispatch valve of the gasoline tank in the tank farm is compromised by an attacker.

Three pressure sensors and three flow rate sensors were used to observe the system state. Sensors were positioned at the inlet and outlet of each centrifugal pump, and at the inlet of the loading arm of the tanker truck. Figure 10 shows the normal flow rate (kl/h) at three distinct locations during a cargo transfer operation. The flow rates at the inlet and outlet of the pump rise almost instantaneously and attain a steady state value of 270 kl/h. Since the tanker truck is located some distance away from the pump house, the rise in the flow rate at the tanker truck gantry is delayed. When the cargo reaches the tanker truck, the initial rush produces a spike in the flow rate, which is followed by a drop to the steady state flow rate of 270 kl/h at the loading arm.

Figure 11 shows the measured pressure values at three locations. The pump inlet has the lowest steady state pressure of 1.18 bar while the pump outlet has the highest pressure of 1.8 bar. The difference in pressure is due to the boost provided by the centrifugal pump. After the cargo reaches the pipeline, it starts losing pressure as it travels along the pipeline. When it reaches the tanker trunk gantry, a lower steady state pressure of 1.6 bar is measured at the loading arm. Note that the spikes in pressure measured by the three sensors at the start of the cargo transfer operation are due to the pressure build up in the pipeline.

During the simulated injection attack, the attacker compromised the motor operated valve in the dispatch pipeline of tank TK 12. The valve was toggled three times during the cargo operation, creating spikes in the flow rate and pressure that are unsafe for pipelines and valves. A Python script using the `pymodbus3` library was used to craft the injection packets. A separate attack node, a virtual machine running Kali Linux, was added to the network connecting the human-machine interface and programmable logic controller. The commands to open and close the valves were sent to the programmable logic controller from the attack node. The attack node injected packets every 50 ms. The human-machine interface was configured to send commands that set the states of all the actuators, including the valve, every 500 ms. During each attack session, the attacker closed the valve, waited for two seconds and then reopened the valve. Because the attacker sent commands at a faster rate and the valve has a relatively high latency to open and close, a command to set the valve actuator state sent by the human-machine interface was overridden quickly by the attacker node.

During the first injection, between 37 and 39 seconds, a spike in the flow rate is observed at all three sensors (Figure 12). Similarly, pressure values of 13.2 bar and 11.2 bar are measured at the tanker truck pump outlet and pump inlet, respectively. Since the dispatch valve of the gasoline tank is closed during

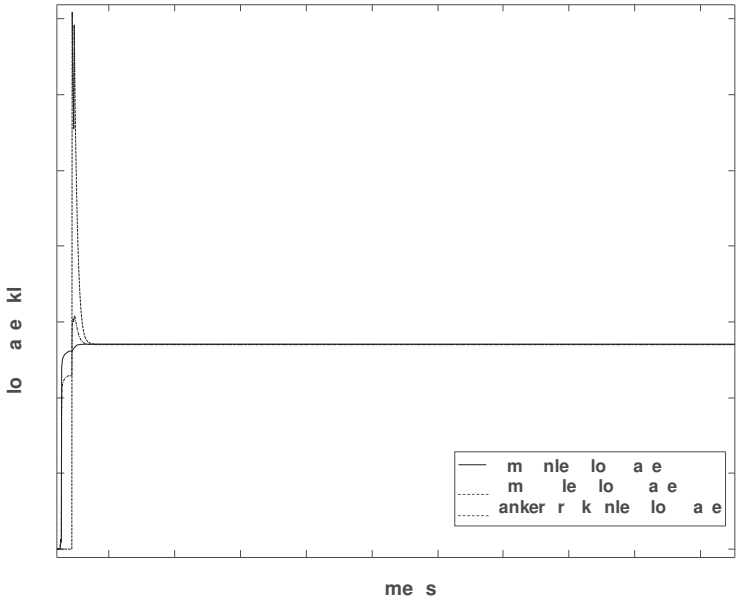

Figure 10. Tanker truck loading flow rate (normal conditions using a single pump).

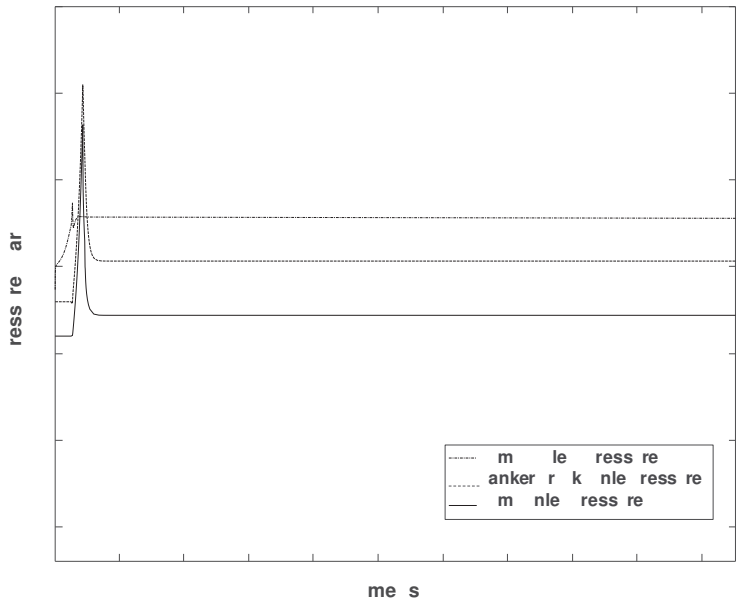

Figure 11. Tanker truck loading pressure (normal conditions using a single pump).

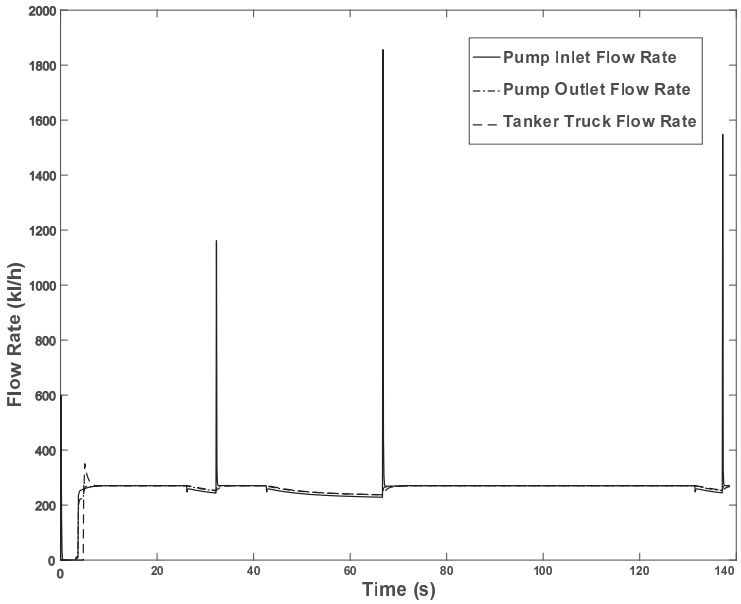

Figure 12. Tanker truck loading flow rate during an injection attack.

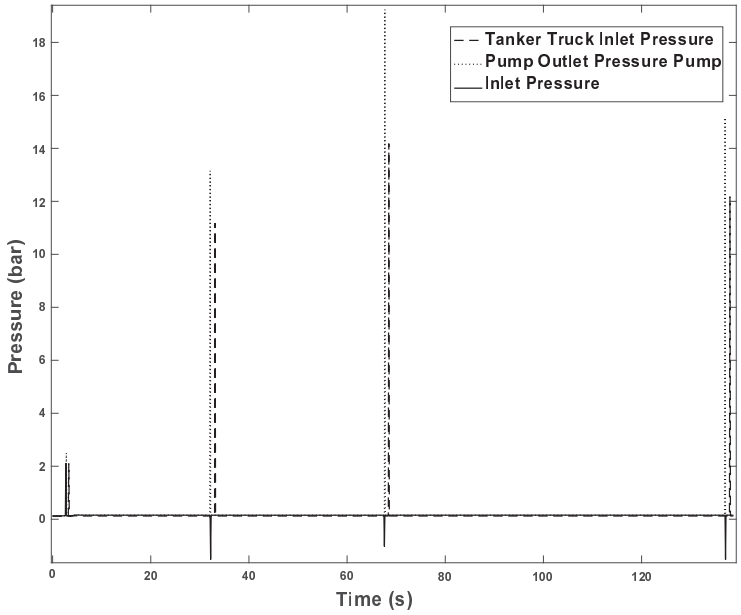

Figure 13. Tanker truck loading pressure during an injection attack.

the attack, the pump creates a negative pressure in the inlet pipeline as shown in Figure 13.

The same injection attack was repeated twice as shown in Figures 12 and 13 between 67 and 69 seconds and between 137 and 139 seconds. During each attack session, the attacker managed to create pressure and flow rate spikes. In the second attack session, the attacker managed to create a very high pressure of 19.8 bar and a flow rate of 1,800 kl/h. Such a high pressure in a closed pipeline system is extremely unsafe and can result in a pipeline rupture.

The injection attack scenario involved an attack on a motor operated valve in the tank farm and the impacts were observed across multiple components of the system. Such a scenario is especially interesting to cyber security researchers because it enables an analysis of the impacts on interdependent components in a midstream oil terminal. In fact, the attack scenario is similar to what occurred in Baku-Tbilisi-Ceyhan pipeline incident [15]. Pressure spikes followed by negative pressure can cause a pipeline to crack or rupture, resulting in the release of hazardous material and, potentially, a fire or explosion.

6. Conclusions

A failure in a midstream oil terminal can result in a catastrophic incident with significant losses of life and property. Cyber threats to critical infrastructure assets such as a midstream oil terminal are dramatically increasing in their number and sophistication. The virtual midstream oil terminal testbed described in this chapter can be used to study cyber security vulnerabilities, examine the impacts of cyber attacks on cyber and physical components, evaluate the effectiveness of security controls and support education and training efforts.

The virtual midstream oil terminal testbed is a large-scale, simulation of multiple interconnected industrial control systems. The entire testbed and all the simulations were executed on a personal computer with an Intel I7 6700K 2,400 MHz processor, 16 GB RAM and a 500 GB solid-state drive running the Windows 10 operating system. Indeed, the virtual midstream oil terminal testbed demonstrates that large-scale models of industrial control systems for cyber security research, education and training are both feasible and valuable.

References

[1] U. Adhikari, T. Morris and S. Pan, WAMS cyber-physical testbed for power system cybersecurity study and data mining, *IEEE Transactions on Smart Grid*, vol. 8(6), pp. 2744–2753, 2017.

[2] T. Alves, OpenPLC Project (`www.openplcproject.com`), 2018.

[3] T. Alves, R. Das and T. Morris, Virtualization of industrial control system testbeds for cybersecurity, *Proceedings of the Second Annual Industrial Control System Security Workshop*, pp. 10–14, 2016.

[4] American Petroleum Institute, Specification for Electric Motor Prime Mover for Beam Pumping Unit Service, API SPEC 11L6, First Edition, Washington, DC, 1993.

[5] American Petroleum Institute, Specification for End Closures, Connectors and Swivels, API SPEC 6H, Second Edition, Washington, DC, 1998.

[6] American Petroleum Institute, Specification for Line Pipe, API SPEC 5L, Forty-Third Edition, Washington, DC, 2004.

[7] American Petroleum Institute, Specification for Bolted Tanks for Storage of Production Liquids, API SPEC 12B, Fifteenth Edition, Washington, DC, 2008.

[8] American Petroleum Institute, Specification for Pipeline Valves, API SPEC 6D, Twenty-Third Edition, Washington, DC, 2008.

[9] American Petroleum Institute, Loading and Unloading of MC 306/DOT 406 Cargo Tank Motor Vehicles, API RP 1007, Washington, DC, 2011.

[10] American Petroleum Institute, Line Markers and Signage for Hazardous Liquid Pipelines and Facilities, API RP 1109, Fifth Edition, Washington, DC, 2017.

[11] C. Bronk and E. Tikk-Ringas, The cyber attack on Saudi Aramco, *Survival: Global Politics and Strategy*, vol. 55(2), pp. 81–96, 2013.

[12] M. Cintuglu, O. Mohammed, K. Akkaya and A. Uluagac, A survey of smart grid cyber-physical system testbeds, *IEEE Communications Surveys and Tutorials*, vol. 19(1), pp. 446–464, 2017.

[13] Independent Inquiry Committee, Independent Inquiry Committee Report on the Indian Oil Terminal Fire in Jaipur on 29th October 2009, Ministry of Petroleum and Natural Gas, Government of India, New Delhi, India, 2010.

[14] International Chamber of Shipping, Oil Companies International Marine Forum and International Association of Ports and Harbors, *International Safety Guide for Oil Tankers and Terminals*, Witherby and Company, London, United Kingdom, 2006.

[15] R. Lee, M. Assante and T. Conway, Media Report of the Baku-Tbilisi-Ceyhan (BTC) Pipeline Cyber Attack, ICS Defense Use Case (DUC), SANS Industrial Control Systems, SANS Institute, Bethesda, Maryland, 2014.

[16] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga and S. Hariri, A testbed for analyzing security of SCADA control systems (TASSCS), *Proceedings of the Conference on Innovative Smart Grid Technologies*, 2011.

[17] J. Mirkovic and T. Benzel, Teaching cybersecurity with DeterLab, *IEEE Security and Privacy*, vol. 10(1), pp. 73–76, 2012.

[18] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu and R. Reddi, A control system testbed to validate critical infrastructure protection concepts, *International Journal of Critical Infrastructure Protection*, vol. 4(2), pp. 88–103, 2011.

[19] M. Nasir, S. Sultan, S. Nefti-Meziani and U. Manzoor, Potential cyber-attacks against global oil supply chain, *Proceedings of the International Conference on Cyber Situational Awareness*, 2015.

[20] Office of Aircraft Services, *Aviation Fuel Handling Handbook*, CreateSpace, Seattle, Washington, 2015.

[21] B. Reaves and T. Morris, Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems, *International Journal of Critical Infrastructure Protection*, vol. 5(3-4), pp. 154–174, 2012.

[22] Y. Zhou, X. Zhao, J. Zhao and D. Chen, Research on fire and explosion accidents of oil depots, *Chemical Engineering Transactions*, vol. 51, pp. 163–168, 2016.