

**SEMESTER 4, ACADEMIC YEAR 2018/2019**

**SKJ 3113**

**INTERNET AND NETWORK SECURITY**

**TITLE:**

**IIoT IN OIL AND GAS INDUTRY**

**LECTURE GROUP:**

**KSC**

**NAME OF LECTURER:**

**Dr Sundrean**

**NAME OF GROUP:**

**MUSA AND HIS FRIENDS.**

**MEMBERS OF THE GROUP:**

|  |  |  |
| --- | --- | --- |
| NUM. | NAME | MATRIC NUMBER |
| 1 | Musa Bojang | 1170001 |
| 2 | Ahmad Izzudin Bin Abdullah Zawawi | 1170070 |
| 3 | Muhammad Atif Bin Ridzuan | 1170032 |
| 4 | Ahmad Fadzil Bin Hafizi | 1171307 |
| 5 | Muhammad Anwar Arif Bin Mohd khir | 1170072 |

**ABSTRACT**

A breakthrough that will revolutionize how industries operate is found in the IIoT. The massive interconnection of intelligent devices aimed at gathering information to make a sound decision is crucial in many industry-like workforces. We believe that the most important technology that is expected to transform many future aspects is the Internet of things. In this paper, we intend to examine the various strengths of the IoT technology with regards to the Oil and Gas industry. We outline several features of the technology that will affect the industry and several security measurements to ensure data integrity, confidentiality and assurance. In this paper, we will illustrate main features of the IIoT and provide recommendation on how to enhance security vulnerabilities.

**INTRODUCTION**

It would be a bit of an understatement to say that the oil and gas industry has had a tough couple of years. Today, public observation is that oil and gas companies are not keeping up with the times. Not only are organizations, like [Google](https://www.inc.com/kevin-j-ryan/google-100-percent-renewable-energy-2017.html?cid=search), spearheading clean energy projects that threaten oil and gas, but other industries are also adopting new technology at faster paces. From [robotics](https://www.inc.com/quora/how-robots-will-run-the-luxury-hotels-of-the-futur.html?cid=search) to [artificial intelligence](https://www.inc.com/nicolas-cole/the-future-of-sales-is-in-artificial-intelligence-.html?cid=search), organizations across verticals recognize that in order to stay relevant among consumers, they have to change with the times. The oil and gas (O&G) industries could benefit a great deal from these new technologies.

Time has come for companies within these fields to revamp their operations and propel themselves to the modern-day playing field. The O&G industry has experienced turbulent times in the last couple of years, and in front of low oil prices, the Companies in the sector have made large efforts toward significant cuts in cost and reduction in the activity of new projects development. Based on the uncertainties about the Industry directions, there have been many speculations about the continuity of petroleum as the main source of energy in the modern civilization and about the permanence of low oil prices for an extended period. Analyses of the usual practices in the Oil & Gas Industry suggests that the sector should pass by a technological reorganization of its methods and industrial processes.

One central theme emerges to be the main catalyst of change which is the Internet of Things (IoT). The Internet of Things (IoT) is poised to fundamentally change the way a wide range of industries approach the procurement, processing, and distribution of raw materials and finished products. New efficiencies based on the introduction of intelligent sensors, mission-critical communications, automation, and robotics will optimize industries ranging from mining and shipping to manufacturing verticals including electronics, automotive and petrochemical products. This emerging megatrend is alternatively called the Fourth Industrial Revolution and Industry 4.0.

Several prospective models indicate that the petroleum, as an energy source, will become obsolete at some point in the future. The big question that challenges researchers around the World is when this energy source replacement will take place in a consistent and definitive way. Considering that the development of any basic infrastructure for a new energy source may require decades, it can be expected that the transition should happen gradually and in a structured manner. Therefore, the most likely Vision to occur is the incorporation of new technologies to make petroleum energy cleaner and more efficient, to allow a gradual change in the energy matrix by the introduction of renewable energies.

Considering the increase in the quality of life in the developing countries, it is expected that the demand for energy will continue to grow, regardless of which energy sources will be used to meet this demand. Based on the current reality, it is believed that the Oil & Gas Industry will retain its leading position in the global energy matrix for a long period. Whereas the production capacity of a field invariably decreases if no action of maintenance or increase of production capacity is performed, it is expected that soon the demand will again overcome the supply, which will generate pressure on prices, making viable field developments that are not commercially attractive today.

Because of the large engineering efforts and time required to develop new fields, there is an inertia to achieve an overall production increase, thereby maintaining the attractiveness for new developments over a period of several years when the demand keeps higher than the supply. However, since all projects begin to operate in successive waves, the supply again exceeds the demand, leading to inventories increase and fall in oil prices again, which is reflected in a seasonal behavior between supply and demand.

On the other hand, one cannot disregard the facts about global warming and the potential environmental risks promoted by the Oil & Gas Industry. Given the difficulties of incorporating new technologies abruptly in the energy matrix, it is imperative that methods and processes of exploration and production should evolve to make the industry more efficient and to minimize its potential environmental impacts. In this context, the needs of the Oil & Gas Industry meet the technological revolution wave provided by Industry 4.0.

**HOW DOES IIOT CONTRIBUTE TO THE O&G INDUSTRY?**

The IIoT is part of a larger concept known as the Internet of Things (IoT). The IoT is a network of intelligent computers, devices, and objects that collect and share huge amounts of data. The collected data is sent to a central Cloud-based service where it is aggregated with other data and then shared with end users in a helpful way. The IoT will increase automation in homes, schools, stores, and in many industries. The application of the IoT to the manufacturing industry is called the IIoT (or Industrial Internet or Industry 4.0). The IIoT is promised to revolutionize manufacturing by enabling the acquisition and accessibility of far greater amounts of data, at far greater speeds, and far more efficiently than before. Several innovative companies have started to implement the IIoT by leveraging intelligent, connected devices in their factories.

Like many other industries, the oil and gas industry is undergoing a rapid[digital transformation](https://www.inc.com/jeff-pruitt/how-does-your-leadership-define-transformation.html?cid=search). Unlike many other industries, however, oil and gas companies have been slow to adopt technological innovations on the software front. Many of the reasons that the industry is slow to evolve are understandable; the capital that was once plentiful has seen a rapid decline and the industry is stuck in the "old way" of doing things

The oil and gas industry, combined, are multi-billion-dollar industries; big oil is big money and the time is now to bring the industry into the digital age. The following are top technologies that have been adopted in other industries yet have been slow to integrate into the oil and gas industry.

**Robotics**: The industry was slow to adopt the use of robotics before 2014, but now companies climbing out of the collapse are implementing them. For example, Iron Roughneck, which was developed by a company calledNational Oilwell Varco Inc[.](http://www.bloomberg.stfi.re/news/articles/2017-01-24/robots-are-taking-over-oil-rigs-as-roughnecks-become-expendable?sf=kevajbr&utm_source=Triggermail&utm_medium=email&utm_campaign=Post%20Blast%20%28bii-iot%29:%20Singapore%20to%20test%20autonomous%20trucks%20%E2%80%94%20Ford%20looks%20to%20branding%20with%20its%20new%20hire%20%E2%80%94%20Robots%20in%20oil%20and%20gas%20enhance%20safety&utm_term=BII%20List%20IoT%20ALL#ab), automates the dangerous and repetitive tasks of connecting drill pipes on oil rigs.

While technologies like these do add value to the companies, there is potential for workers to lose their jobs, which is a recurring fear that many have when it comes to robots.

Chris Blackford, the founder of [Sky-Futures](https://www.sky-futures.com/), a drone company for the oil and gas industry, [explained](https://www.ft.com/content/74418aac-3a06-11e5-bbd1-b37bc06f590c#axzz44heJIf2I) that "the inspection data we can collect in five days takes rope-access technicians about eight weeks."

**Artificial Intelligence**: In the oil and gas industry, AI allows companies to uncover trends that pinpoint and predict inefficiencies. Leveraging AI to improve performance operations from C-level to field worker, automate processes, streamline manual business operations, and connect with IoT devices, makes every arm of the company more efficient and profitable.

"To survive the current era of cheap oil, we will see the democratization of tools like AI, automation, and IoT. The oil and gas sector must capitalize on such business intelligence, otherwise, they will undoubtedly be left behind in a worldwide digital revolution," says Rajagopalan.

**Cloud Computing**: As the oil and gas undergo this enormous transformation to a digital infrastructure, cloud computing will prove to be a powerful engine. The sheer amount of data companies can harness and further analyze through automation, will reduce operational expenses, down well times, and lessen risk. As more oil and gas companies integrate cloud computing, this will empower field workers to optimize production.

"To take effective action, the entire production chain, from COO right down to on-site well engineers, need to see the very detailed cost and production data, narrowed down to the invoice level. By leveraging cloud computing capabilities, accuracy and transparency are achieved in the shortest amount of time to drastically improve well-cost management," explains Rajagopalan.

Even industries that aren't traditionally progressive can no longer afford to staunchly opposed change and digital transformation. Luckily for organizations that may have been slow to adapt, emerging technologies, including cloud computing, AI, and robotics can be easily implemented and impactful almost immediately.

In the fourth Industry revolution, 'Data' should and will play a role in O&G. The IIoT can greatly improve connectivity, efficiency, scalability, time savings, and cost savings for industrial organizations. Companies are already benefitting from the IIoT through cost savings due to predictive maintenance, improved safety, and other operational efficiencies. IIoT networks of intelligent devices allow industrial organizations to break open data silos and connect all of their people, data, and processes from the factory floor to the executive offices. Business leaders can use IIoT data to get a full and accurate view of how their enterprise is doing, which will help them make better decisions. The question is how we can utilize existing data to yield valuable and reliable conclusions to pave the way for new direction. Key would be to make sense of the data, try to make apple to apple comparisons, looking for trends, determine what data is useful and which is not. This may help develop similar models as used in Real Time Optimization (RTO) for manufacturing plants balancing process conditions and an economic model that helps to maximize profit or reduce costs.

**IoT devices**

The devices involved with the IoT technology are numerous. We understand that IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the internet, and they can be remotely monitored and controlled. Khaleel and Pilar (2018, p. 25) mentions in the citation of (Cata, 2015) that authors recommend a model for a smart university, which is consisted of utilizing sensor devices in the five main categories namely Environment sensors used to detect noise, temperature and lightening, Security sensors for motion detection, opening/closing doors or windows and fingerprints, Safety sensors to detect smoke, fire, and water, Utilitarian sensors for electrical voltages and NFC tags and Information sensors for RFID cards, QR tags, and barcodes. All the above-mentioned devices and many more constitute what we now call the IoT technology.

All the connected devices, in the IoT network, are part of a scenario in which every device communicates to other related devices, including the above mentioned devices, in an environment to automate home and industry tasks, and to communicate usable [sensor data](http://internetofthingsagenda.techtarget.com/definition/sensor-data) to users, businesses and other interested parties. IoT devices are meant to work in concert for people at home, in industry or in the enterprise. As such, the devices can be categorized into three main groups: consumer, enterprise and industrial.

**Technological developments in the Oil and Gas Industry.**

Like any industries out there, the O&G industry faces a lot of changes. The Oil and Gas industry is going through massive disruption and, as we continue to be extremely dependent of these organic sources of energy, we should consider looking at the emerging new macro and micro trends affecting this global industry. The Oil and Gas industry investments in the energy revitalization will continue to shift. It is observed that new innovative trends will flow from the upstream sector to midstream infrastructure, refinery operations, and petrochemical facilities. The Upstream operators in the oil and gas industry will focus on harvesting value from recent discoveries and acquisitions through more efficient operations, looking at measuring the risks the industry is facing and the application of new technologies and innovations. It is easy to see how technology is reinventing retail, entertainment, healthcare, telecommunication, but there’s little discussion of technology’s impact on the universe of companies and industries focused on natural resources extraction, such as petroleum, oil and gas.

As stated earlier, the Oil and Gas industry can benefit a great deal from these technologies. But one may ask, what is stopping them from leveraging the strength of it. According to Andrew Medal (n. d), the Oil and Gas industries are slow to adapt to new technologies. He argues Many of the reasons that the industry is slow to evolve are understandable; the capital that was once plentiful has seen a rapid decline and the industry is stuck in the "old way" of doing things.

However, there is need for the O&G industry to adapt to new technologies especially the IoT due to the following reasons. The basic premise is a web-based visualization platform from which companies can manage, measure and track all the data coming from all over the oilfield. This is provided by software technology. We also know that the development of seismic imaging in three dimensions greatly changed the nature of natural gas exploration. This technology uses traditional seismic imaging techniques, combined with powerful computers and processors, to create a three-dimensional model of the subsurface layers. 4-D seismology expands on this, by adding time as a dimension, allowing exploration teams to observe how subsurface characteristics change over time. Exploration teams can now identify natural gas prospects more easily, place wells more effectively, reduce the number of dry holes drilled, reduce drilling costs, and cut exploration time. This leads to both economic and environmental benefits.

Another technological advance we have seen in past couple of years is coiled tubing. Coiled tubing technologies replace the traditional rigid, jointed drill pipe with a long, flexible coiled pipe string. This greatly reduces the cost of drilling, as well as providing a smaller drilling footprint, requiring less drilling mud, faster rig set up, and reducing the time normally needed to make drill pipe connections. Coiled tubing can also be used in combination with slim hole drilling to provide very economic drilling conditions, and less impact on the environment.

Furthermore, the IoT technology can do even better. With the approaches of cloud computing and big data, we realize it could contribute a lot to the industry. David Farr (2018, p) believes that the good news has just begun to flow for oil and gas companies. That's because the opportunities for applying technologies that bring down costs and boost productivity are still enormous, and innovation is expanding rapidly. The turnaround we have begun to see in some companies' fortunes is only the tip of the iceberg.

Another interesting aspect of the IoT infrastructure is the big data. With various sensors deployed, it has the ability to measure not only variables such as temperature, pressure and fluid levels, but also more sophisticated ones, like corrosion, vibration and hazardous leaks. Coupled with the ability to wirelessly communicate all these measurements reliably, it saves vast sums on engineering, no-longer-necessary wiring and labor. They can communicate over the Industrial Internet of Things (IoT), which is no longer a dream – it's a reality. But this innovation is just beginning.

Now consider the ability to access the quantities of information – the Big Data – that all these tireless sensors are producing. Cloud computing makes it possible to set up central operations wherever we want, even as the sensors operate in "four D" environments – places that are Dull, Distant, Dirty and Dangerous. New software and analytics are enabling companies to chew the Big Data into digestible bites and give them actionable insights. As a result, companies can predict, save and optimize in ways that would have been considered impossible only a few years ago.

**IIOT TRANSPORTATION IN GAS AND OIL INDUSTRY**

Oil and Gas is a multibillion-dollar industry because the product they possess has a high demand. This leads our discussion as to how effective and reliable is the transportation system of the O&G industry. Oil and natural gas combined [provide over half of the world’s energy](http://www.forbes.com/sites/quora/2013/04/03/what-are-the-top-five-facts-everyone-should-know-about-oil-exploration/#59336606127d). In near run, traditional methods of transporting oil and gas will become old-schooled because the IoT is promising a smart transport in which the transporter is on constant monitor. We explain how improvements can be made with the help of IIoT in transportation with regards to O&G industries.

Gassing up your car for the weekend, listening to the steady flow of fuel as it moves from the pump into the car’s tank, it’s easy to overlook the journey of those hydrocarbons — their birth at a remote offshore oil well more than 500 feet below the surface, being battered by turbulent waves in transport across the rugged North Pacific, only to find themselves traveling hundreds more miles in a pipeline across searing desert terrain.

A stop at the refinery and then they were off again, carried by train and truck until finally arriving at your local filling station. Along the way, they passed through countless pumps, holding tanks, meters, monitors and hoses. A failure at any one of those points, at any stage in a journey made countless times every day around the world, may have ruined your weekend.

To serve the continuous demand for fuel and oil all over the globe, the petroleum supply chain buzzes 24 hours a day, from some of world’s most remote areas to its most accessible. Many of the equipment involved in mining, moving, refining and selling it is expensive, and rugged, and comes from hundreds of manufacturers.

With so many variables, finding a way to monitor these expensive capital assets and use that data to improve efficiency, drive better performance, enable innovation and keep fuel flowing has always been a major challenge for the oil and gas industry. This is where the IoT comes in.

Enhanced by the [Internet of Things](http://internetofyourthings.com/) (IoT), Rockwell Automation, which is an [American](https://en.wikipedia.org/wiki/United_States) provider of industrial [automation](https://en.wikipedia.org/wiki/Automation) and [information technology](https://en.wikipedia.org/wiki/Information_technology), is bringing its vision for The Connected Enterprise to life by building new forms of intelligence to transform the petroleum supply chain. This is expected reaped the bottom-line results in global productivity and competitiveness that could ultimately pay off at the pump.

Doug Weber, business manager, remote application monitoring for Rockwell Automation, describes the vision with potential of delivering a degree of collaboration and visibility unheard of in the oil and gas industry. With help of sensors, software and the cloud, these disparate assets can become part of a Connected Enterprise, powered at its core by a rich flow of data.

Founded in 1903 with a line of machine controllers, today Rockwell Automation is using Microsoft’s IoT services to extend its business and provide managed monitoring and support for its products in the field. The company has put years of research into developing cloud-based solutions, using software, sensors and devices to predict equipment failures along the supply chain, track its performance in real time, and help refine designs and processes to prevent those failures in the future.

Oil and natural gas are necessary resources. A lack of oil and natural gas would have the country (and the world) grinding to a halt. Though there have been “renewable” and “sustainable” energy initiatives, none of them have been able to contribute a significant amount of energy to the world. They have either been prohibitively expensive, difficult, or simply unreliable. Oil and natural gas run the world, and without it many countries would not be able to sustain their daily operations.

**TRANSFORMING DOWNSTREAM TRANSACTIONS**

While the oil and gas industry provide the lifeblood of transportation, it is also dependent on it. Getting the crude out of the ground is one thing, but once it’s out, it must be moved to refineries and ultimately to the pump. Accomplishing this is a vast network of ships, barges, pipelines, trains and trucks crisscrossing the globe.

At nearly every intersecting point in this network, there is a piece of equipment familiar to those in the industry that most people would never think about: The so-called “skids” that measure the amount of product transferred from one container to another as it changes hands.

Known as Lease Automatic Custody Transfer (LACT) units, these skids have historically been just one of thousands of assets scattered around the world and often located in the middle of nowhere. Doing their jobs in isolation with no connectivity, skids have traditionally relied on paper-based processes and periodic site visits for routine maintenance, leaving them vulnerable to inaccuracies and failures — until a company called [Trigg Technologies](http://www.triggtechnologies.com/) changed that with the help of Rockwell Automation and Microsoft.

By modernizing LACT units with sensors and moving that information to the cloud with Azure, Trigg Technologies has enabled its skids for remote service and maintenance, including the ability to monitor the product being transferred to ensure it is correct, and coordinate immediate electronic invoicing.

Soon, the ability to automate these transactions across thousands of machines and countless miles is transformational for this industry. Now all parties involved can have immediate electronic records of transactions, real accountability in these remote locations, immediate awareness for maintenance and diagnostics, and new levels of information about every transaction.

**BUILDING A SMARTER GAS PUMP**

Hundreds of miles downstream and on street corners around the world is another piece of equipment that most people are familiar with: retail gas pumps. While most people use these for gasoline, today many delivery trucks are fueled by liquid natural gas, and so pumps designed to handle that fuel source are making their way to filling stations worldwide as well.

One major oil company is working with local gas stations to install liquid natural gas fueling lanes, and they’re taking it a step further, partnering with Rockwell Automation, to connect and cloud-enable the new pumps.

Cloud gateway appliances at each station collect the data and securely send it to a cloud platform provided by Rockwell Automation. Collecting and storing real-time data from hundreds of sensors, variable frequency drives and Rockwell Automation’s control systems allows each of the stakeholders across their supply chain to perform their function more efficiently: “On a basic level, there are reports on the functioning of the equipment, inventory of fuel, consumption rates, and analytics to predict when they’ll need to perform preventive maintenance, replenish supplies, etc.,” Weber says. “This drives significant productivity and cost savings.”

Rockwell Automation uses Azure to provide the resulting dashboards as a Web application that can be viewed on PCs, iPhones, Windows Phones or Android devices. According to Weber, this flexible platform allows various entities involved with the operation to access the information and put it to use.

As the project moves along, Weber says, the volume of data collected could facilitate predictive analysis to better anticipate imminent failures and maintenance needs. The data can also be used to improve the design of pumping stations and other equipment based on that long-term perspective. To facilitate these innovations, Rockwell Automation is beginning to tap into [Azure Machine Learning](http://azure.microsoft.com/en-us/services/machine-learning/) to understand how the massive amounts of data being collected can create even more value.

“The more data we have, the more we can learn and put together algorithms to predict problems,” says Weber. It’s about taking information from that control system and using it to make those systems even more efficient and productive.

**A VAST NETWORK OF PIPELINES AND EFFECTS OF RUPTURES AND LEAKS**

In the US and many other developed countries, around 55,000 miles of crude oil trunk lines connect regional markets. Oil wells connect to this backbone through 40,000 miles of gathering lines. And the end products of refineries travel through 95,000 miles of pipelines.

The U.S. Energy Information Administration stated that there are some 305,000 miles of interstate and intrastate natural gas transmission pipelines in the US, with an additional 1.25 million miles of natural gas distribution pipeline.

Pipelines are everywhere. You've probably passed over a buried pipeline many times and never knew it. Pipelines carry crude oil or natural gas over land. It used to be that oil sold by the barrel would be hauled by horse-drawn wagons to the railroad where they were transported for a longer journey. This is where we get our unit of measurement for oil being sold. One barrel these days equals roughly 42 gallons.

There are a series of different pipes that carry oil and gas from beginning to end that you could imagine is similar to a tree with roots, a trunk and branches. Oil pumped fresh from the ground is pumped into collector pipelines. From the collector pipelines they are pumped to field processing stations where larger pipes push the material to a main-line pipeline.

This main-line pipeline is most often a larger pipe and will carry the product to refineries many miles away. From here the refinery will pump the material through a series of smaller pipelines that divide into smaller branches until they reach distribution depots.

The pipelines are mostly coated steel pipe buried underground. Oil pipelines typically transport liquid at pressures between 600 and 1000 psi, while natural gas pipelines go up to 1500 psi (per square inch). These high pressures are why ruptures can be so serious, and why monitoring and detecting flaws in advance is so important, particularly given the age of some of these pipes. The US Department of Transport (DOT) reports that more than half are at least 50 years old.

It is only when there is a leak in pipelines the public tend to be conscious, leading to a toxic spill, or even an explosion that costs lives. Yet pipelines are by far the safest way to move large amounts of petroleum, and really the only way to transport natural gas. But an accident, when it happens, can be serious. While a derailed tanker train can only spill as much oil as it is carrying, a ruptured pipeline can continue to pump. Thus, prompt detection and shutdown are essential.

Alex Jablokow(2015, p) mentions that the industry has started the incorporation of sensing technologies to monitor the pressure, flow compressor condition, density, temperature and other variables. This is because ruptures often start as pinhole leaks, that visual inspection can easily miss until they become serious and detrimental. Acoustic sensors can detect a breach by a variation in the acoustic signature. Fiber optic sensors detect deformations in the pipe walls.

Sensors are also sent down the pipes for inspection. The most popular is a robotic instrument called a smart pig. The name comes from the squealing noise the original models, wire-wrapped straw used for cleaning out wax and other contaminants, made as they traveled down the pipe. Depending on the model, smart pigs detect cracks and weld defects through magnetic flux leakage or shear wave ultrasound, mechanically measure the roundness of the pipe to detect crushing, or measure pipe wall thickness and metal loss through compression wave ultrasound.

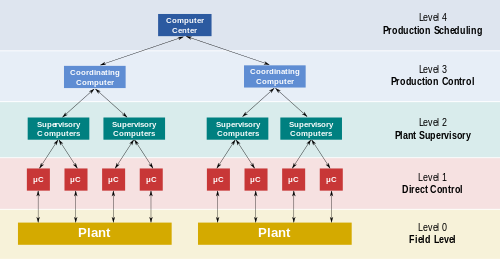
Smart Pigs or Pipeline Inspection Gauges are large pieces of machinery pulled together with powerful technology that help with the maintenance of transmission pipelines. These pipeline pigging devices are major components to pipeline safety and accident prevention.  These inspection tools provide data on the condition of [pipelines](http://www.smartpigs.net/pipelines.html) which help gauge the health and integrity of the pipes. In a time where environmental protection is key and of global concern, smart pigs are the peacekeepers of the delicate relationship between pipelines and Mother Earth (and regulators). In addition, these smart pipeline pigs make sure that transmission of the product doesn't stop due to pipeline integrity issues, which can be disastrous to the bottom line. High-quality pipeline construction is integral as these pipes operate under immense pressure. One leak can cause a massive explosion. Luckily, smart pigs are capable of diagnosing problems that can lead to these environmental disasters before they happen.

In General, Smart Pigs are used to detect stress corrosion cracking, general and pitting corrosion. In specific: gouges, dents, pit corrosion, anomalous weld seams, longitudinal cracks, longitudinal grooves, and general corrosion are all detectable.

If you've ever had an MRI (An MRI is suited for examining soft tissue in ligament and tendon injuries, spinal cord injuries, brain tumors etc..) or know what one is then you can imagine a pipeline pig very similarly. These often two-ton objects are equipped with highly tuned sensors that can gauge the thickness of the pipes they are traveling through along with cracks, fissures, erosion and other problems that may affect the integrity of the pipeline. Data is collected and transmitted to a team that interprets that data to gauge the health of the pipeline segments being scanned. If any problems are found, then teams not only know what the problem is thanks to a heavy set of data points but know exactly where to go to replace the affected pipe thanks to highly tuned sensors.

**FROM SCADA TO IOT**

The system that integrates this information on an operational level is called SCADA (Supervisory Control and Data Acquisition). SCADA is a [control system](https://en.wikipedia.org/wiki/Control_system) architecture that uses computers, networked data communications and [graphical user interfaces](https://en.wikipedia.org/wiki/Graphical_user_interface) for [high-level](https://en.wikipedia.org/wiki/High-level) process [supervisory management](https://en.wikipedia.org/w/index.php?title=Supervisory_management&action=edit&redlink=1), but uses other peripheral devices such as [programmable logic controller](https://en.wikipedia.org/wiki/Programmable_logic_controller) (PLC) and discrete [PID controllers](https://en.wikipedia.org/wiki/PID_controller) to interface with the process plant or machinery. The operator interfaces that enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA computer system. However, the real-time control logic or controller calculations are performed by networked modules that connect to the field sensors and [actuators](https://en.wikipedia.org/wiki/Actuators).



The accompanying diagram above is a general model which shows functional manufacturing levels using computerized control.

Referring to the diagram,

* Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as [control valves](https://en.wikipedia.org/wiki/Control_valve).
* Level 1 contains the industrialized input/output (I/O) modules, and their associated distributed electronic processors.
* Level 2 contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.
* Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
* Level 4 is the production scheduling level.

It is used to gather and monitor data and then to do something like turn a valve or change the set point on a flow controller. SCADA is common in industrial operations that require real-time control of system operations.

In industrial implementations, the [Internet of Things](http://www.ptc.com/internet-of-things)  develops on top of the already existing system, allowing for a move from “monitor and respond” to a predictive and proactive approach supporting improved decision making.

Over the past five years, Pacific Gas & Electric (PG&E), which operates 6,700 miles of gas transmission pipeline and 42,000 miles of gas distribution pipeline in northern and central California, has worked intensively to become predictive and proactive in the way it manages its network.  According to Mel Christopher, Senior Director of Gas Systems Operations, this will be a multistep journey. These steps can serve as a model for all such IoT implementations.

**Situational awareness** creates intelligence out of the data, with better visualizations that enable operators in the Gas Control Center to see changes in the system quickly.

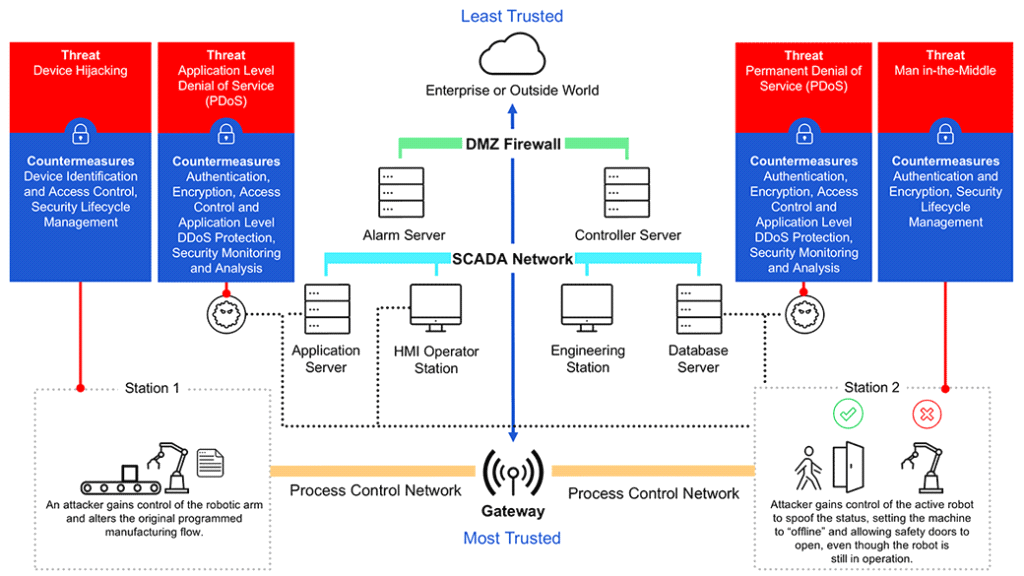
**Situational intelligence** follows, and integrates geospatial and temporal data to give a precise understanding of specific events as they happen.

**Predictive analytics** finally take all of that real-time data and pull out patterns that signal approaching abnormal events, allowing for proactive responsiveness.

**SAFETY AND SECURITY ISSUES OF IIOT**

Vulnerabilities are present everywhere throughout variety of systems, regardless of a system’s scale of operation, data capacity and network traffic volume. A small blunder or mishap in certain parts of a system could set the domino effect into motion that’ll greatly implicates other parts of an intricate system. This unfortunate turn of event would gradually drag the system’s performance and expose the bulk of the system to outside breaches that such the chain reaction of system malfunctions might also be orchestrated and caused by third-party interference. In short, even a slight mistake or distortion could cripple an impenetrable, impregnable and security-critical system causing influxes of trust issue among the clients and employees of such a “horridly-desingned” system so as not mention the huge repair bills amounting on the desk of the executives. Similar things could be uttered for IIoT, since it’s fundamental idea is to heavily relied on high-degree of interconnection between the sets of sensors, actuators and etc. The very concept of the IIoT could be used to go against it, as smart devices dependent on constant feedbacks from other devices to cooperate and operate, the attackers could exploit it to the fullest by either by severing the connection between the interconnected devices or sending false data feedbacks to the devices or eavesdropping on the communication between the devices to attain vital data so that it can be used for further attacks.

Cyber threats are mainly targeted at the Industrial Control Systems (ICS), such as the Distributed Control Systems (DCS); Supervisory Control and Data Acquisiotion (SCADA) systems; Programmable Logic Computers (PLC) and Human Machine Interfaces (HMI). Furthermore, following the introduction of IP-based connectivity to be used as the communicational link between multiple industrial devices has drastically elevate the concerns regarding security risks. This ever increasing and creeping possibilities of threats had caused numerous distrust amongst the oil giants to integrate and enhance their operations using IIoT concept since the unknown was not made clear and encountered effectively. If the situation remains, this could haphazardly jeopardize the chances of technological improvements and benefits that could be bring forth by the wave of IIoT integration so as to hinder the IIoT future breakthroughs altogether. So to speak, on public level, this situation appeared to be not needing any desperate urge or massive widespread of awareness as it wouldn't directly effect the mass public, but still on the hindsight or according to human developmental view, this situation is perilous on it's own unique way. This part of the report would descriptively discuss on countermeasures or techiques that were suggested by the IT professionals or know-hows so that the knowledge could be applied and implemented to combat malicious and endearing cyberattacks on IIoT infrastructure and it's incorporated devices.



The following are some common or rather possible attacks and threats posed to the IIoT architecture of oil and gas industry.

a) **Man-in-The-Middle:**

The “Data is the New Oil,” quote is used to explain the increased value of exploding “gushers” of personal and organizational information that can transform customer experiences and business processes. And ironically, the “new oil” quote is usually used to describe transformations in industries other than the massive one that is occurring in the oil and gas industry. The reality is that there is no industry in which the quote “data is the new oil” is truer than in oil and gas. Central to surviving – and thriving – in this unstable era is reinventing an organization’s information strategy

The man-in-the-middle attack happens when an attacker manages to breach, interrupt or spoof communicational links between two or more systems. In the context of an IIoT scenario, an attacker might be able to assume control of a smart actuator and knock an industrial robot out of its designated lane and speed limit - which arises the potential of damaging an assembly line or injuring operators who're supposed to maintain the machine's integrity.

b) **Device Hijacking**:

Actively happens when the attacker hijacks and assumes control of a device effectively so as holistically. This type of attack is highly difficult to be detected prematurely due to the action of the attacker to not change the basic functionality of the device. Furthermore, the potential to might as well infect other unaffected devices, for example, smart meters that are connected to the grid. Generally, according to an IIoT scenario; a hijacker could gain enough control of a smart meter and utilize the compromised device to launch staunch ransomware attacks against Energy Management Systems (EMSs) or illegally siphon unmetered power lines.

c) **Distributed Denial of Service (DDoS):**

A denial-of-service is a variant of attack (DoS attack) in hope to render a machine or network resource to be unavailable or unreachable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed denial-of-service attack (DDoS), influx of traffic flooding a target originates from multiple unclarified sources, elevating the difficulty to abruptly halt the cyber offensive by simply blocking a single source. DoS and DDoS attacks can negatively affect a wide range IIoT applications, causing critical disruptions for utility services and manufacturing facilities.

**ATTACKS ON ROSNEFT AND OTHER OIL GIANTS**

A known and well-positioned Russian O&G Mogul, Rosneft and Evraz were recently victims of a massive cyber-attack conducted by anonymous group of hackers whose motives were unknown. The attack caused Rosneft's company servers to go abuzz, luckily the attack did not inflict any physical damage or disrupt its oil production capability. The malicious code named NotPetya was the culprit as it infiltrated the servers, demanded ransom to be paid to regain access to the system. The Petya variant, NotPetya commonly targets Microsoft Windows-based systems, the ransomware infected the master boot record to execute a payload that encrypts a hard drive's file system table and prevents the Windows from booting or shutting down. This ransomware troublesome appearance scouts a never-ending and impeding problem for companies across the world and uncover the baffling question to fully ensure the safety of corporate data of accumulated by companies.

**COUNTERMEASURES AND PREVENTATIONS**

All of the infrastructure in relation to IIoT have to be shielded using a cyclopedic security solution (device-to-cloud) that doesn't break out any disruption to the operations, amenity, dependability or economic accountability. Rather than opting for a 'super solution' that horribly unsuccessful in gaining any noteworthy traction, a more profound, simplistic, yet secure solution that is able to be incorporated vastly and with ease by IIoT operators and their respective amenities is extensively more acceptable. The capabilities that should be present in a solution follows:

i) **Firmware robustness and assured boot**

To make sure that an appliance does only run code synthesized by the appliance OEM or another trustworthy party, the secure boot must apply cryptographic code signing techniques. The practicality of of implementing the utilization of assured boot technology inadvertently stops hackers from substituting firmware with malevolent instruction sets, abruptly eliminating any attempt of attacks. Sadly, there are some of IIoT chipsets aren't equipped with secure boot capabilities. Generally, it is crucial to assure that IIoT appliances can only establish communicational link with authorized amenities to prevent any endangering possibility of substituting firmware with spinful instruction sets.

ii) **Reciprocal authentication**

Before receiving or transmitting data, a smart actuator will try to establish a connection to the network, so every time the smart actuator attempts to do that, it should be authenticated. This practical countermeasure safely assures the data is coming from a legitimate appliance and not an illicit source. For two-way verification, the utilization of the asymmetric keys or symmetric keys that are involved in the cryptographic algorithms are supplementary. In a brief example, the Secure Hash Algorithm (SHA-x) along with the Hash-based Message Authenticated Code (HMAC)can be applied for symmetric keys and Eliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys.

iii) **Assured Communicational link (end-to-end encryption)**

Assured and safe communicational link potentiality secure data in transit between an appliance and its amenities infrastructure (the cloud). By using encryption, the secrecy of the data transmitted is kept to those only who're permitted and intended to by supplying the intended receiver the decryption key. Such an example is, the communication between a smart actuator and SCADA, that sends usage data, should be able to preveny itself from the potential digital eavesdropping.

iv) **Safeguarding surveillance and inspection**

For the security observation, it basically seizes data on the holistically state of an industrial system, that involve endpoint appliances and connectivity traffic. The data is then inspected and probed if there is any occurrence or possibility of any security violations or suspected system threats. Immediately after detecting a threat, there will be a multitude of actions already composed in the context of a holistically system safeguarding policy should be implemented, this is done by such the action of revoking appliance qualifications or quarantining an IoT appliance based solely on abnormal performance. To probe usage behaviors and spot suspected attack scenarios, the automatic principle of monitor-analyze-act cycle may execute in the real time or at a postponed period. Therefore, the vitality or cruciality of ensuring of safeguarding the endpoint of appliances from any unwanted risk of notorious tampering or data manipulation would not be compromised, for this unfortunate occurrence will trigger arrays of incorrect reporting event.

**CONCLUSION**

In conclusion, the IIoT concepts have transform the Oil & Gas industry business model in fast and dramatic ways since the connectivity is now widespread and huge volumes of process data are being delivered to the cloud for management. Besides, the cost of connected sensors has plummeted, allowing Oil & Gas companies to accelerate digitization programs and to leverage a higher mobility of work force. All this factors have a big impact to the growth of industry nowadays, not only in Oil & Gas industry, but also in other industry like transportation, medical and others. When an industry involves in IIot, security and safety are something that need prioritize since it will impact the profit and loss in the industry. There are various kind of attacks like Man-in-the-Middle, device hijacking and DDoS, and all those kind of attacks are very common in IIoT. Therefore, the industry need to take the countermeasures in order to avoid the problem from happening to increase the efficiency and production of industry.

**REFERENCES**

* David Farr. ‘ New Technologies will fuel surging US Oil Production’, *CNBC* [online]. Available at https://www.cnbc.com/2018/03/05/new-technologies-will-fuel-surging-us-oil-production-commentary.html(Accessed: 5 March 2018)
* Khaleel Mershad & Pilar Wakim (2018) ‘A Learning Management System Enhanced with Internet of Things Applications’, *Journal of Education and Learning, Vol 7,p.23-29.*
* <https://blogs.microsoft.com/iot/2014/12/04/fueling-the-oil-and-gas-industry-with-iot/>
* [Alex Jablokow](https://www.ptc.com/en/blog-authors/Alex-Jablokow) (2015). ‘*Industrial Internet of Things’.*PTC[online] Available at <https://www.ptc.com/en/product-lifecycle-report/how-the-iot-helps-keep-oil-and-gas-pipelines-safe>
* SmartPigs (n.d), ‘*Pipeline Pigging with Smart Pigs* [online]. Available at [www.smartpigs.net/](http://www.smartpigs.net/)
* https://www.techrepublic.com/blog/it-security/ddos-attack-methods-and-how-to-prevent-or-mitigate-them/
* <https://www.computerweekly.com/news/252443327/CDO-interview-Andrei-Belevtsev-Gazprom-Neft>
* <https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/>
* <https://www.rambus.com/iot/industrial-iot/>