SAP Cybersecurity for Oil and Gas

Alexander Polyakov

Matheu Geli

Disclaimer

The partnership agreement and relationship between ERPScan and SAP prevents us from publishing the detailed information about vulnerabilities before SAP releases a patch. This review will only include the details of those vulnerabilities that we have the right to publish as of the release date. However, additional examples of exploitation that prove the existence of the vulnerabilities are available in conference demos as well as at ERPScan.com.

Our SAP security surveys and research in other areas of SAP security do not end with this whitepaper. You can find the latest updates about the statistics of SAP services found on the Internet and other endeavors of the EAS-SEC project.

Intro

The idea is simple. We want to show that mission-critical business applications are often connected between each other using different types of integration technologies. What's more important, enterprise applications which are located in the corporate network are usually connected with devices in OT network and there is no easy way to separate them.
If you have some plant devices which collect data about oil volumes, for example, you should somehow transfer this data to the corporate network to demonstrate it on nice dashboards to management. That's why even if you have a firewall between IT and OT there are some applications which are connected. That is why it's possible to conduct such attack and pivot from IT network (or even the Internet) into OT network up to field devices and smart meters.

What else?

- It is the first Oil and Gas Cybersecurity research ever so far.
- There are still more questions than answers in this area. The more detailed research requires unique equipment. However, there are many software and hardware devices which are relatively easy to find if you really want.
- It is just a beginning. Our goal was not to write a comprehensive encyclopedia on Oil and Gas cybersecurity but to lay the basis for further research (that hopefully will be conducted by the community) and to show that all issues in technology networks that we have already discovered (and you will) can be exploited from the corp network. So we welcome everybody to continue this research.

Who should read this white paper and why?

- Researchers – Oil and Gas Cybersecurity is a small universe which is almost unexplored. If you have ever thought about doing something in this area, here is your chance to spend 2 hours instead 2 months, as after reading this paper, you will definitely know what to do to carry out your own research.
- Pentersters - you will learn how to break into the most critical network and how to impress decision makers during your pentests. Instead of "Hey, we have access to your domain controller" you will be able to say something like: "Hey, I can change the gas pressure in your storage. Isn't it critical enough?"
- CISOs – There are is a bad news, unfortunately. Now you will learn that there is no Air Gap between your enterprise network and Oil Refinery, sorry. The truth is that hackers can pivot into your production systems from the corp network or even from the Internet. This paper will help you to understand how to prevent it
- SAP and Oracle admins – You guys are partly responsible for the security of very important OT processes. SAP and Oracle Systems have connections with most of those systems by one or another way. This whitepaper will highlight what exactly can be wrong.

Why Oil and Gas?

We have chosen Oil and Gas sector because of 2 things:

1) We have an experience and understanding of processes as we saw them on a real environment and can prove that these attack vectors are possible to be performed (we presented them during our customer engagement)

2) Oil, Gas, and other natural resources are not easy to be measured. To be honest, they are not measurable at all, and it's possible to spoof this data in a way that nobody will be able to investigate.
Let's compare it with the retail industry. You know how many Nike boots are stored in your warehouse and even if somebody has access to it, steals shoes and then changes their quantity in ERP system, in some time someone will find that something is wrong. If you deal with natural resources, nobody knows the real quantity. It's basically calculated on a number of metrics such as pressure, temperature, etc… According to the description of some of the popular technologies which help to optimize Hydrocarbon Supply Chain, hydrocarbon volumes fluctuate depending on environmental temperature and pressure conditions. As product valuation needs quantity and mass, and simple weighing is not possible, one should derive them from volumes at ambient temperature and pressure conditions, requiring complex conversion calculations of the observed volumes at each custody transfer point. Imagine what can happen if an attacker accesses and modifies this data.

Oil and Gas Cybersecurity

Industrial automation and control systems such as SCADA (supervisory control and data acquisition), DCS (Distributed Control System), PLC (Programmable Logical Controllers), OPC servers, Field Devices, and other critical components are often referred to as Operational Technology (OT).

OT is used to monitor and control physical processes in the oil and gas industry. The role of OT is the acquisition of data coming from processes (temperatures, pressures, valve positions, tank levels, human operators) and the direct control of electric, mechanical, hydraulic or pneumatic actuators.

In the good old days, most OT networks were air-gapped from the business network (office network) and the Internet and operated independently using proprietary hardware, software and communications protocols. But in recent years, demand for business insight, requirements for remote network access and the spreading of hardware and software from traditional IT (e.g., TCP/ IP networking, Windows-based platforms) caused many oil and gas companies to integrate control systems and their enterprise IT systems, and some of them can even provide an access to OT network from the cloud.

Cybercrimes cost energy and utilities companies an average of $13.2 million each a year for lost business and damaged equipment, higher than in any other industry, according to Ponemon's survey of 257 businesses. [1]

Oil and Gas Cybersecurity history

December, 2002 - Venezuela's state oil company became embroiled in a bitter strike. There were also instances of computer hacking which caused a significant damage since many operations are centrally controlled by computers. Someone, possibly an employee involved in the general strike, remotely accessed a program terminal to erase all PLC programs in port facility. This and other physical sabotage cut Venezuela's national production down to 370,000 barrels per day, compared with 3 million barrels before the strike.

2008 - Hackers interfered with alarms and communications for Baku-Tbilisi-Ceyhan pipeline in Turkey, super-pressurizing crude oil to cause an explosion that resulted in the spilling of more than 30,000 barrels of oil.

23 October, 2009 - An explosion happened in Bayamon, Puerto Rico. The fire blazed for three days, burning down houses and causing black clouds of gasoline-fueled smoke and forcing residents to flee their homes. Investigators said it was a glitch in the facility's computerized monitoring system. A storage tank was getting refilled with gasoline from a fuel ship docked along the San Juan harbor. Since the tank's meter malfunctioned, the petrol kept overflowing until it met an ignition source. [2]

2010 - STUXNET was used to hijack industrial control systems around the globe, including computers used to manage oil refineries, gas pipelines, and power plants. Although Stuxnet was not designed for Oil and Gas, it seriously affected these companies as well.

2012 – As a result of cyber attack on Aramco, Saudi Arabian national petroleum and natural gas company, 30000 computers were damaged. The attack aimed to stop gas and oil production in Saudi Arabia and prevent resource flow to international markets.

10 September, 2012 - Telvent is a supplier of remote administration and monitoring tools to the energy sector became a victim of sophisticated advanced persistent threat. Its Canadian branch discovered on September, 10 that its internal firewall and security systems had been breached and notified its customers of the incident.

According to Telvent, every energy company in the Fortune 100 relies on their systems and information to manage their business. Telvent systems now manage more than 60 percent of the total hydrocarbon movements in North American and Latin American pipelines.

The likely attacker appeared to be a Chinese hacking group. The malware names and network components used in the attack have been used in the past by a Chinese cyber-group called the "Comment Group," according to Dell SecureWorks. Comment Group has targeted a variety of organizations, including chemical and electric companies as well as other industrial sectors.

After breaching the network and installing malware, the attackers stole project files related to the OASyS SCADA product, a remote administration tool. OASyS allows companies to combine older IT equipment with modern "smart grid" technologies.

The attackers may have wanted the code in order to find vulnerabilities in the software to launch future attacks against other energy companies directly. [3]

January, 2015 - A device used to monitor the gasoline levels at refueling stations across the United States—known as an automated tank gauge or ATG—could be remotely accessed by online attackers, manipulated to cause alerts, and even set to shut down the flow of fuel, according to research. Several Guardian AST gas-tank-monitoring systems have suffered electronic attacks possibly instigated by hacktivist groups. Successful attacks can affect inventory control, data gathering, and delivery tracking, in turn impacting the availability of gasoline in local stations. [4]

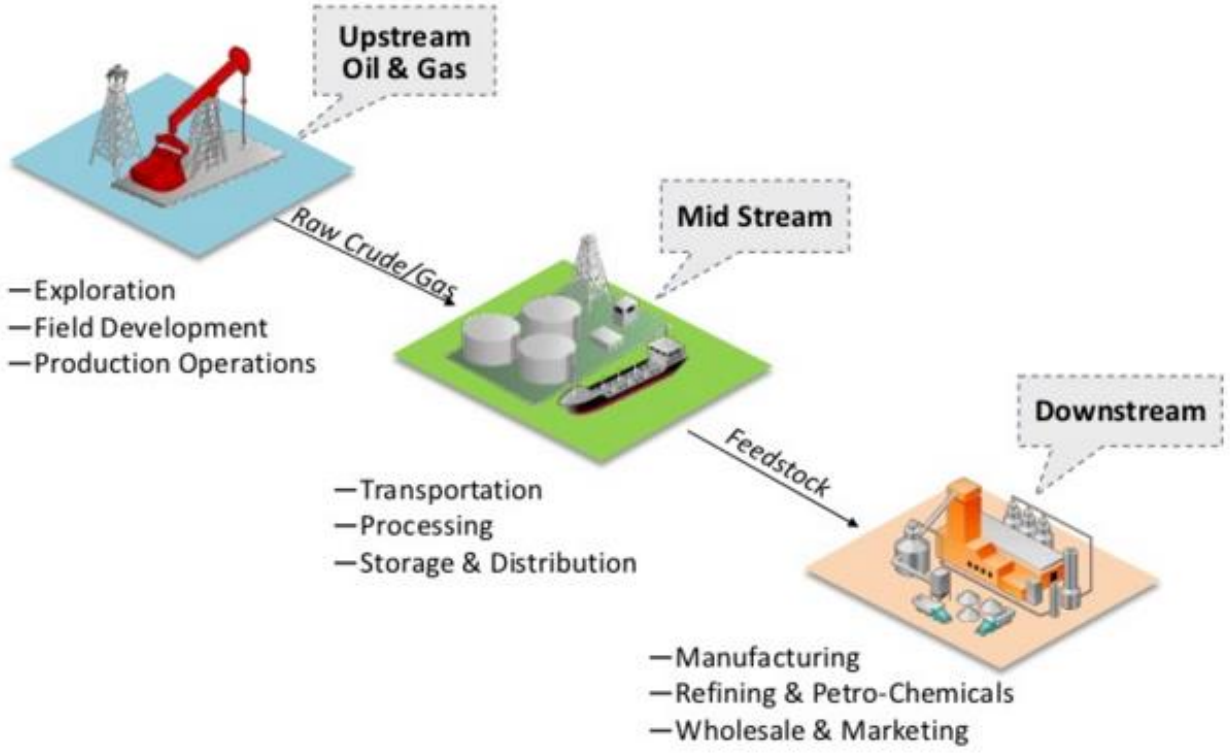
Oil and Gas 101

Oil and Gas processes are usually divided into 3 separate areas: Upstream, Midstream, and Downstream.

Upstream - The upstream sector includes the searching for potential underground or underwater crude oil and natural gas fields, drilling of exploratory wells, and subsequently drilling and operating the wells that recover and bring the crude oil and/or raw natural gas to the surface. The upstream oil sector is also commonly known as the *exploration and production (E&P) sector*.

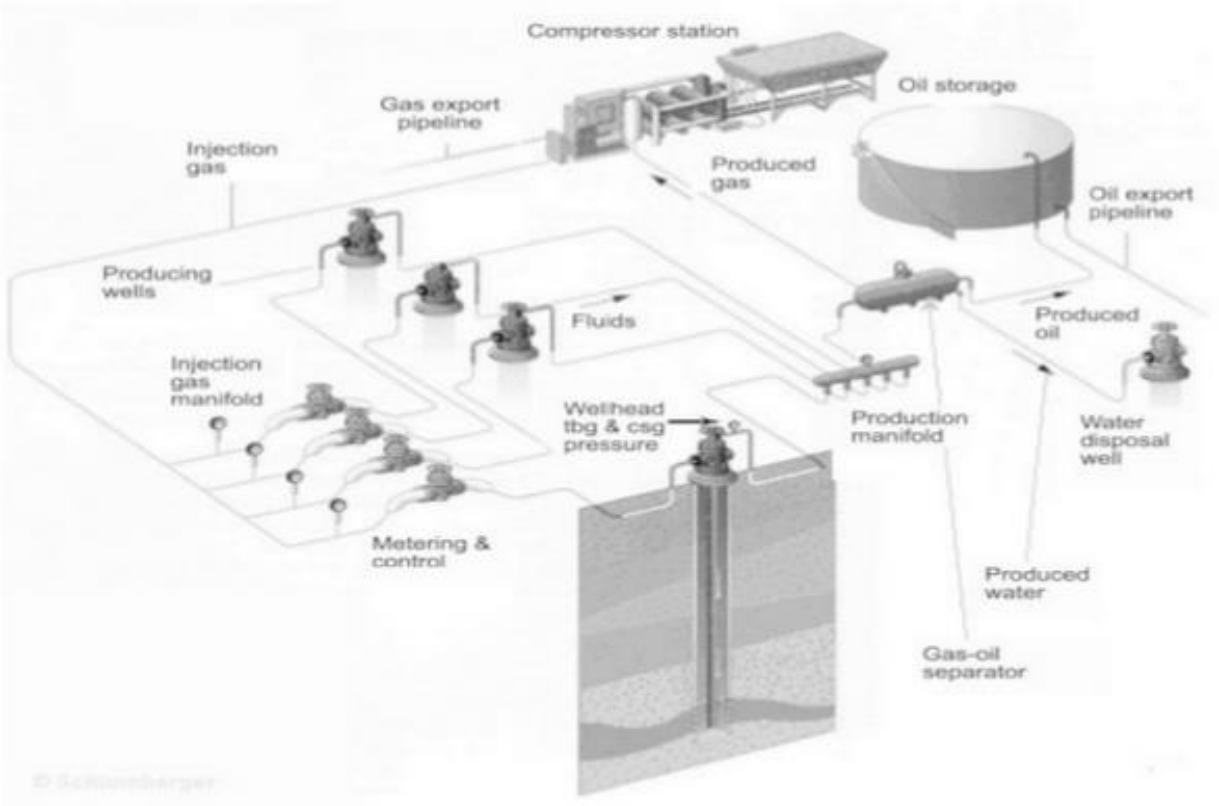
Midstream- The midstream sector involves the transportation (by pipeline, rail, barge, oil tanker or truck), storage, and wholesale marketing of crude or refined petroleum products. Pipelines and other transport systems can be used to move crude oil from production sites to refineries and deliver the various refined products to downstream distributors.

Downstream -The downstream sector commonly refers to the refining of petroleum crude oil and the processing and purifying of raw natural gas, as well as the marketing and distribution of products derived from crude oil and natural gas. The downstream sector touches consumers through products such as gasoline or petrol, kerosene, jet fuel, diesel oil, heating oil, fuel oils, lubricants, waxes, asphalt, natural gas, and liquefied petroleum gas (LPG) as well as hundreds of petrochemicals. [5]



Upstream

The upstream segment of the business is also known as the exploration and production (E&P) sector which encompasses activities related to searching for, recovering and producing crude oil and natural gas.



Simple Upstream oil and gas process

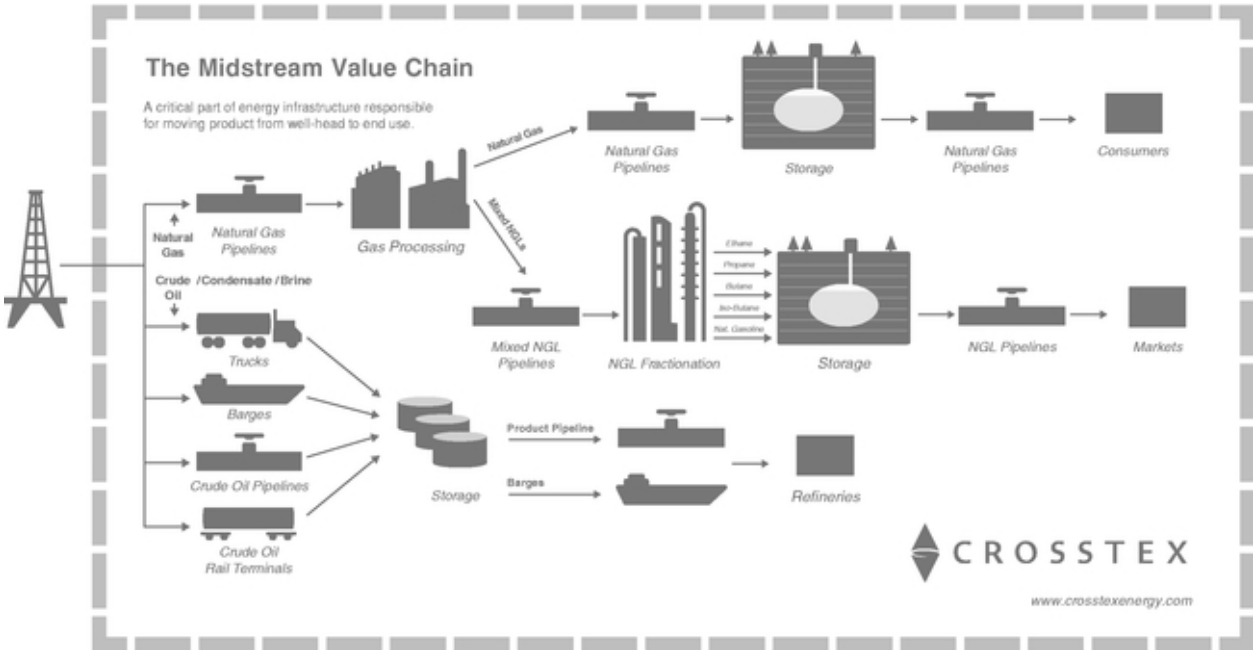
Upstream consists of the following main business processes which, in their turn, consist of listed sub-processes:

- Extraction (Drilling)
  - Pump control, blow-out prevention, flaring, and venting
- Gathering (From earth to separators)
  - Wellhead management, manifolds management, net oil measurements
- **Separation (Separate oil, gas and water)**
  - Multiple separators (2phase/3phase), Heaters, **Burners**, Coalescence, Desalting
- Gas compression (Prepare for storage and transport)
  - Multiple stages
- Temporary Oil Storage (Temporarily store before loading)
  - Tank Inventory System, Movement management
- Waste disposal
  - Water disposal
- **Metering (Calculate quantity before loading)**

- **Fiscal Metering**, Liquid Flow Metering, Gas Flow Metering Systems, Wet Gas Metering Systems, Provers & Master Meters

Midstream

The midstream sector involves the transportation (by pipeline, rail, barge, oil tanker or truck), storage, and wholesale marketing.



Midstream consists of the following main business processes which, in their turn, consist of listed sub-processes

- **Terminal management (Obtain Oil from Upstream)**
  - Measurement, Automation, Order Movement Management
- **Gas Processing (Separate natural gas and NGL)**
- **Gas Transportation (transfer gas to storage)**
  - Pipeline management
- **Oil transportation (transfer Oil to storage)**
  - Pipeline management
- **Gas storage (temporary and long-term)**
  - Peak load Gas Storage, Gas storage, LNG Storage
- **Oil Storage (Long-term oil storage)**
  - Tank inventory system, Tank Temperature management, Tank Gauging System, Product Movement

Downstream

The downstream sector commonly refers to the refining of petroleum crude oil and the processing and purifying of raw natural gas, as well as the marketing and distribution of products

derived from crude oil and natural gas.

Downstream consists of the following main business processes which, in their turn, consist of listed sub-processes:

- Refining (Processing of Crude Oil)
  - Blend Optimization, Emission Monitoring System
- Oil Petrochemicals (Fabrication of base chemicals and plastics)
  - Too many processes to be listed here
- Gas Distribution (deliver Gas to utilities)
- Oil Wholesale (deliver petrol to 3rd party)
  - Loading, Terminal automation
- Oil Retail (deliver petrol to end-users)
  - Truck loading Automation, Gas-Pump-Monitoring-Systems, POS

Critical Processes

Extraction (Drilling)

Drilling is physically creating the "borehole" in the ground that will eventually become an oil or gas well. This work is done by rig contractors and service companies in the Oilfield Services business sector.

It consists at least of the following sub-processes:

- Pump controll
- Blow-out prevention - Subsurface safety valve is installed to prevent Blow-out
- Flare and Vent disposal

Extraction as a business process was not covered in this research.

Gathering

Risk: Plant Sabotage/Shutdown, Compliance violation, **Equipment damage**, **Production Disruption, safety violation**

Gathering includes all processes responsible for lifting crude oil from the ground and transfering it to separators.

Well monitoring systems

Wellheads are situated on the surface of oil or gas wells leading down to the reservoir. Wellhead can also be an injection well used to inject water.

Well monitoring systems (WMS) are used to estimate the flow rates of oil, gas and water from all the individual wells in an oil field. The real-time evaluation is based on data from available sensors in the wells and flow lines.

Manifolds management

The individual well streams are brought into the main production facilities over a network of gathering pipelines and manifold systems.

Net Oil Measurement

Sometimes, Oil measurement starts here just to estimate values.

Invensys Foxboro is one of the examples of solutions which can be used here. [6]

Separation

Risks: Product Quality, Equipment damage

Oil generally comes out of the well mixed with water and, often, small amounts of natural gas. Similarly, natural gas often comes out of the ground mixed with water vapor and other gasses. These various components must be separated before "pipeline quality" oil and/or natural gas can be sent to market.

To remove water and natural gas from oil, the mixture is passed through a device that removes the gas and sends it into a separate line. The remaining oil, gas and water mixture goes into a heater/treater unit. Heating helps to break up the mixture so that oil separates from water, which is denser. Any remaining natural gas, which is less dense than oil, rises to the top. The gas is removed for either processing or burning; water is removed and stored for further treatment.

Additional separation of oil from wastewater is accomplished using hydrocyclones. Hydrocyclones spin the oil/water mixture, and use acceleration to separate oil from water. Water is forced to the outside of the hydrocyclone, where it is removed. Because most wastewater is very salty, it cannot be used as a water resource. Instead, it is injected back deep into the subsurface, usually into the same formation where the oil and water came from, helping force more oil out of the reservoir.

One promising new separation technology is the freeze-thaw/evaporation (FTE) process. Using a freeze crystallization process in the winter and natural evaporation in the summer, wastewater is separated into fresh water, concentrated brine, and solids. Offshore, the salty water is tested to make sure that it does not contain any oil or other impurities that could hurt sea life, and is then put into the ocean.

Burner Management System (BMS)

In the oil and natural gas industry, various facilities (e.g. tanks, line heaters, separators, dehydrators, amine reboilers, etc.) are used in the production and transportation of oil and natural gas. They require heat, which is used to facilitate the proper function of the application. To provide that heat, a burner is used within the application.

Burner Management Systems help to make oil & gas companies safier, more efficient, and more compliant.

Without a BMS, companies will face the following problems:

- Worker must discover and reignite the extinguished burner. The worker then reignites the application manually (often with a fuel-soaked rag that’s tied to a stick). This process takes time and can be very dangerous.
- No electronic temperature control. The application burns continuously, often needlessly, until the flame fails.
- No safety shutdown (with BMS certain application inputs (e.g. high/low pressure, level, etc.) indicate a potential problem).

Most of the major ICS vendors provide BMS solutions.

Examples of BMS systems:

- Invensys BMS [7]
- Emerson DeltaV SIS BMS [8]
- Siemens BMS [9]
- Honeywell BMS [10]

Separators consist of many other sub-processes controlled by the following systems, to name a few:

Distributed Control System

For example, CENTUM CS3000 by Yokogawa.

Emergency Shutdown System (ESD)

For example, Emerson DeltaV SIS™ Emergency Shutdown

Compressor Control System (CCS)

For example, Three Triconex TS3000 TMR

Vibration Monitoring System (VMS)

For example, Bently Nevada 3500

Waste disposal

Risk: Plant Sabotage/Shutdown, Utilities Interruption, Compliance violation

Water disposal

Water disposal and related processes were not covered by this research.

Metering

Risks: Product Quality, Monetary loss

Metering is the most significant process. It's very critical as the quality of final products depends on how proper the metering was. During the metering, systems analyze density, viscosity water content, temperature, and pressure. The metering usually consists of several runs. Each run employs one meter and several instruments for temperature and pressure correction. Gas metering is less accurate than Oil metering (+-1%). The most important part of metering is fiscal metering.

Custody Transfer (Fiscal Metering)

Custody Transfer in the oil and gas industry refers to the transactions involving transporting physical substance from one operator to another. This includes the transferring of raw and refined petroleum between tanks and tankers, tankers and ships and other transactions. Custody transfer in fluid measurement is defined as a metering point (location) where the fluid is being measured for sale from one party to another. During custody transfer, accuracy is of great importance to both the company delivering the material and the eventual recipient, when transferring a material.

The term "fiscal metering" is often interchanged with custody transfer, and refers to metering that is a point of a commercial transaction such as when a change in ownership takes place. [11]

Payment is usually made as a function of the amount of fluid or gas transferred, so accuracy is paramount as even a small error in measurement can add up fast, leading to financial exposure in custody transfer transactions. For example, Pump Station 2 on the Alaska Pipeline is designed to pump 60,000 gallons per minute (227 cubic meters per minute) of oil. A small error of 0.1% equates to an error of 2,057 barrels of oil a day. At a spot price of $105 a barrel, that 0.1% error would cost $216,000 a day. Over a year, the 0.1% error would amount to a difference of $78.8 million. Note that the error could either be on the high side, benefiting the seller; or on the low side, to the buyer's benefit.

The engine of a custody transfer or fiscal metering installation is the flow computer. It is the device that takes the inputs from the measuring devices (flowmeters, pressure sensors, temperature sensors, density sensors, gas chromatographs, and others) and calculates the amount of liquid or gas that has been transferred. These calculations are based on a variety of industry standard flow calculation algorithms. [12]

Metering control software

Data aggregation and management systems provide the complete information enabling one to gain and maintain control over all aspects of the measurement processes. It gives a basis for important decision-making at all levels, from QMI engineering to top management.

Its predictive maintenance philosophy not only reduces unnecessary work, expense and down time; it primarily eradicates give-away inherent to previous systems.

Examples of Fiscal Metering systems:

Data Aggregation and management (easy to manipulate values)

- FlawCall – FlawCall Enterprise (! Internet access)
- **KROHNE SynEnergy** (! Internet access + SAP Access)
- Honeywell's Experion® Process Knowledge System (PKS), MeterSuite™
- OPC Servers (Keepware, MatrikonOPC) (SAP Access)
- Schneider Electric InFusion
- Schneider Electric SCADAPack

Flow computing: (hard to manipulate)

- KROHNE Summit 8800
- ABB TolatFlow
- Emerson FloBoss S600 (previously known as Daniel DanPac S600)
- Emerson ROC800
- Schneider Electric Realflo

Flow Meters

- KROHNE, Vortex, etc

The most common flow computer is **Emerson Foboss S600** (Previously known as Daniel DanPac secure metering computer Daniel S600+) [13]

The FloBoss S600+ Flow Computer is a panel-mounted (for indoor use) flow computer designed specifically to measure hydrocarbon liquid and gas where versatility and accuracy matter. The standard features of the S600+ make it ideal for fiscal measurement, custody transfer, batch loading, and meter proving applications. The S600+ allows you to configure multi-stream, multi-station applications, enabling you to simultaneously meter liquids and gasses. The S600+ can be used either as a stand-alone flow computer or as a component of the system. The intelligent I/O modules fit both gas and liquid. Adding I/O modules (up to a maximum of three) allows you to configure up to six dual-pulsed streams or up to 10 single-pulsed streams and two headers. The S600+ supports orifice, ultrasonic, turbine, positive displacement, Coriolis, Annubar, and V-Cone® flow. [14]

Gas Processing

Major transportation pipelines usually impose restrictions on the make-up of the natural gas that is allowed into the pipeline. Before the natural gas can be transported, it must be purified. Ethane, propane, butane, and pentanes must be removed from natural gas, but it does not mean that they are all ‘waste products’.

In fact, associated hydrocarbons, known as ‘natural gas liquids’ (NGLs) can be very valuable by-products of natural gas processing. NGLs consist of ethane, propane, butane, iso-butane, and natural gasoline. The complete processing of natural gas takes place at a processing plant, usually located in a natural gas producing region. The extracted natural gas is transported to these processing plants through a network of gathering pipelines, which are small-diameter, low-pressure pipes. A complex gathering system may consist of thousands of miles of pipes, interconnecting the processing plant to upwards of 100 wells in the area.

Gas Processing processes were not covered by this research.

Gas Transportation

A significant part of the data received by a control station is provided by supervisory control and data acquisition (SCADA) systems. These systems are essentially sophisticated communications systems that take measurements and collect data along the pipeline (usually in metering or compressor stations and valves) and transmit the data to the centralized control station. Flow rate through the pipeline, operational status, pressure, and temperature readings may all be used to assess the status of the pipeline at any one time. These systems also work in real time, so there is little lag time between taking measurements along the pipeline and transmitting them to the control station. Equipment status scans are taken every 6-90 seconds depending on the communication technology used in the field (NPC 2001).

This information allows pipeline engineers to know exactly what is happening along the pipeline at all times, which permits quick reactions to equipment malfunctions, leaks, or any other unusual activity along the pipeline, as well as to monitoring load control. Some SCADA systems also incorporate the ability to **operate certain equipment along the pipeline remotely,** including compressor stations, which allows engineers in a centralized control center to adjust flow rates in the pipeline immediately and easily

SCADA systems can also operate on cell phone technology, such as the Cellular Digital Packet Data network, which does not require dedicated lines or other infrastructure such as an antenna tower. Some SCADA systems operate directly through the Internet, eliminating certain maintenance concerns for the operator and adding new risks.

Gas Transportation processes were not covered by this research.

Oil Transportation

Oil transportation Track crude and product movements via pipelines. Oil transportation solutions accurately tracks incoming and outgoing movements via pipelines down to the terminals, enabling more accurate crude unit scheduling.

Oil transportation processes were not covered by this research.

Base load Gas Storage

There are basically two uses for natural gas in storage facilities: meeting base load requirements and meeting peak load requirements.
Natural gas storage is required for two reasons: meeting seasonal demand requirements and as insurance against unforeseen supply disruptions. Base load storage capacity is used to meet seasonal demand increases. Base load facilities are capable of holding enough natural gas to satisfy long-term seasonal demand requirements. Typically, the turn-over rate for natural gas in these facilities is a year; natural gas is generally injected during the summer (non-heating season), which usually runs from April through October, and withdrawn during the winter (heating season), usually from November to March. These reservoirs are larger, but their delivery rates are relatively low, meaning the natural gas that can be extracted each day is

limited. Instead, these facilities provide a prolonged, steady supply of natural gas. Depleted gas reservoirs are the most common type of base load storage facility.

Base load Gas storage processes were not covered by this research.

Peak load Gas Storage

Peak load storage facilities are designed to have high-deliverability for short periods of time, meaning natural gas can be withdrawn from storage quickly should the need arise. Peak load facilities are intended to meet sudden, short-term demand increases. These facilities cannot hold as much natural gas as base load facilities; however, they can deliver smaller amounts of gas more quickly, and can also be replenished in a shorter amount of time than base load facilities. While base load facilities have long term injection and withdrawal seasons, turning over the natural gas in the facility about once per year, peak load facilities can have turn over rates as short as a few days or weeks. Salt caverns are the most common type of peak load storage facility, although aquifers may be used to meet these demands as well.

Peak load Gas storage processes were not covered by this research.

LNG Storage

The LNG storage facility liquefies natural gas by cooling it to -160 degrees centigrade and stores it in liquid form. The key feature is its location and ability to rapidly revaporise the natural gas, and deliver it to the National Transmission System (NTS).

As a result, LNG storage is able to provide a peak gas supply to shippers and supplement NGGs network capacity. In addition, LNG Storage is used as a contingency against the risk of emergencies such as system constraints, failures in supply or failures in end user interruption.

LNG Gas storage processes were not covered by this research.

Oil Storage

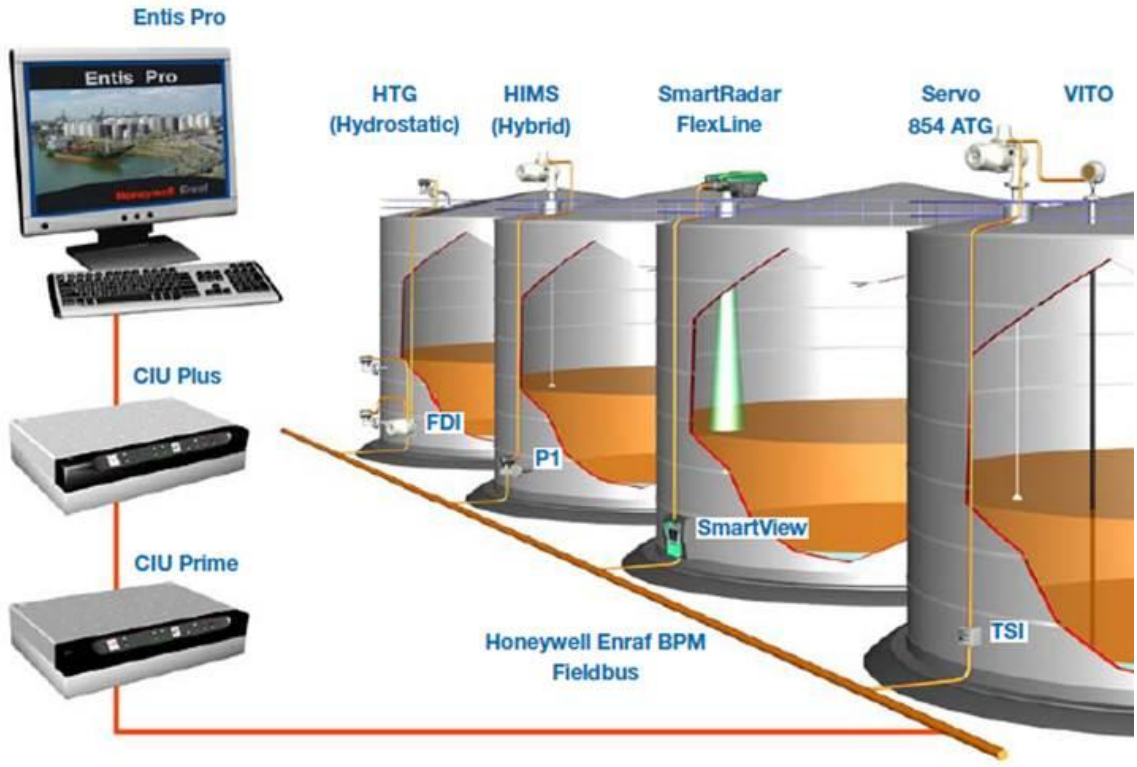
Risks: Plant Sabotage/Shutdown, Equipment damage, Production Disruption, Compliance violation, Safety violation

Oil is stored in storage tanks. Storage location usually consists of 10-100+ tanks with 1-50m barrels. To manage these tanks, companies use Tank Inventory systems. Tank Inventory System collects data from special tank gauging systems such as level, pressure or float radars that are used to measure the level in storage tanks, they also store records of volumes and history.

Monitoring the levels in offsite storage tanks of flammable materials can significantly reduce the likelihood of initiating events that could have a potential impact not only on the operation but also on safety and the environment. Tank level deviations can result in hazardous events **such as a tank overfilling**, liquefied gas flashing through a pressure safety valve header, a floating roof mechanical damage, or an extraction pump running dry. The high severity of consequences for safety and the environment are exacerbated by the large inventories of hazardous materials involved. As more operations are pressed to make improvements in their tank farm and terminal operations management systems, the following offers an overview of best practices for complying with the HSE Recommendations while reducing costs and driving more value from the operation.

Here is the list of most common solutions for Oil and Gas:

- Systems which are connected with IT
  - **Enfaf TM BOX**
  - **Honeywell's Experion® Process Knowledge System (PKS) (For Terminals)**
- Tank Inventory Systems (single-window interface for Tank Gauging Systems)
  - Emerson Rosemount TankMaster WinOpi
  - Schneider-electric SimSci™
  - Honeywell Enraf Entis Pro
  - MHT's – VTW
- Tank Gauging Systems
  - Emerson TankMaster Server
  - Honeywell Enraf BPM
  - Saab, Varec, GSI, MTS, L&J……..
  - Meter Management
  - ControlLogic PLC
  - SmartView
- Meters/Gauges
  - SmartRadar FlexLine
  - ABB
  - Honeywell VIT
  - **Enraf 854 ATG Servo Advanced Tank Level Gauge**



Management consoles of Tank Inventor systems do not just read the data. Some of them such as Emerson Rosemount TankMaster WinOpi can also control Tank Gauging software and hardware. If an attacker gains unauthorized access to control commands, he, for example, can change any Alarm (Level, Temperature, Pressure) for tanks configured as servo tanks or send Freeze and Lock commands to a servo gauge.

Refinery

Risks: Plant Sabotage/Shutdown, Equipment damage, Product Quality, Production Disruption, Compliance violation, Safety violation

The job of the refinery is to sort and improve the hydrocarbons within the crude. Gasoline, propane, jet fuel, heating oil, and petrochemicals are just some of the specially formulated products leaving the refinery. Technicians in a central control room can fine-tune refinery operations to produce the desired mix of products.

An oil refinery, or petroleum refinery, is an industrial process plant where crude oil is processed and refined into petroleum naphtha, gasoline, diesel fuel, asphalt base, heating oil, kerosene and liquefied petroleum gas.

Oil refineries are typically large, sprawling industrial complexes with extensive piping running throughout, carrying streams of fluids between large chemical processing units.

In many ways, oil refineries use a lot of the technology of, and can be thought of, as types of chemical plants. [15]

Refinery solutions are the following:

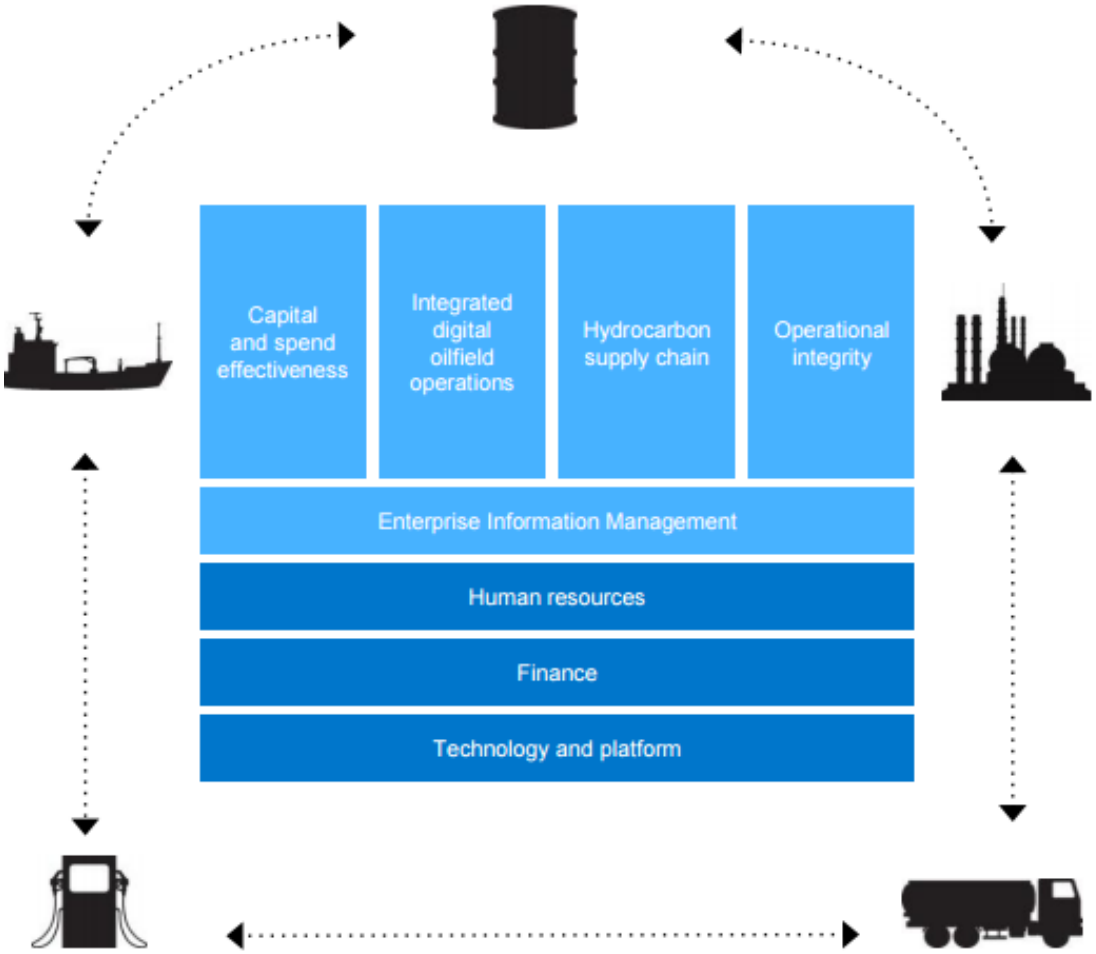
- Solutions for high-level overview and decision-making
  - Emerson DeltaV, **OSISoft PI (Advanced Metering Infrastructure)**
- Management solutions
  - Siemens Simatic SCADA (Lots of vulnerabilities)
  - Experion PKS SCADA
  - Modcon SCADA
  - Ignition SCADA
  - Schneider-electric SimSci™
- Devices
  - Siemens
  - MODCON MOD-800
  - + hundreds of specific devices for each refinery state

Enterprise Applications in Oil and Gas

SAP (ABAP, J2EE Mobile, HANA, BusinessObjects) and Oracle (EBS, PeopleSoft, JDE, Siebel) applications are very common in large companies and especially in the Oil and Gas sector. SAP has more than 246000 customers worldwide including 86% of Forbes 500 and 85% of Fortune 2000 Oil and Gas. Oracle applications are used by 100% of Fortune 100 companies.

SAP in Oil and Gas

Today, upstream operations bring together many technical disciplines and business functions that are loosely connected. The challenge is to support a closed-loop view, ***leveraging a common platform for operations and maintenance,*** *to enable you to gather, analyze, decide, and execute across the many elements that drive performance of assets at different lifecycle stages.*



SAP in Oil and Gas: Capital and Spend Effectiveness

Advantages:

- Improving supplier relations
- Reducing the cost of processing supplier invoices
- Enhance visibility and Transparency

Risks:

- Availability – direct impact on cost effectiveness
- Fraud – price/quantity manipulation
-

Applications:

- SAP PPM

SAP In Oil and Gas: Hydrocarbon Supply Chain

Advantages:

- Hydrocarbon production management
- Hydrocarbon revenue management
- Field logistics

Risks:

- Supply chain Availability – direct impact on cost effectiveness
- Fraud in SAP – Manipulations with quantities*
- Sabotage - Physical damage

Applications:

- SAP ECC IS-OIL

Hydrocarbon volumes, which are the basis for pricing, excise duty, and transportation fees, fluctuate depending on environmental temperature and pressure conditions; as we require masses and weights for product valuation, and weighing is not possible, we must derive them from volumes at ambient temperature and pressure conditions, requiring complex conversion calculations of the observed volumes at each custody transfer point. Different units of measurement are in use globally, further complicating the issue, as even modern terminal automation systems do not support all units of measure – Forrester Research

SAP in Oil and Gas: Integrated Digital Oilfield Operations

Advantages:

- Integrate production, maintenance, and engineering operations
- Streamline data collection, validation, surveillance, and notification
- Close the gap between decision making and on field execution

Risks:

- Sabotage - Physical damage to production and engineering devices
- Operations Availability – direct impact on cost effectiveness
- Data manipulation in SAP – improper management decisions, lost profits

Applications:

- SAP ECC IS-OIL
- SAP PRA (production and revenue accounting)
- SAP RLM (remote logistic management)

SAP In Oil and Gas: Operational Integrity

Advantages:

- Monitor key risk indicators and access control policy
- Maintain the structural and mechanical integrity of physical assets
- Manage emissions, hazardous substances, and product and regulatory compliances

Risks:

- Access control, data manipulation
- Sabotage - Physical damage to production and engineering devices
- Compliance Violation – Manipulation of data to give an illusion of meeting compliance requirements

Applications:

- SAP EAS/PM (Asset Management)

IT applications VS OT processes

Let's look at how business applications are connected with critical OT business processes.

- Enterprise project portfolio management <- Exploration
  - SAP PPM, Oracle Primavera, MS Project, MS SharePoint

- Asset Lifecycle Management <- Refinery, Separation

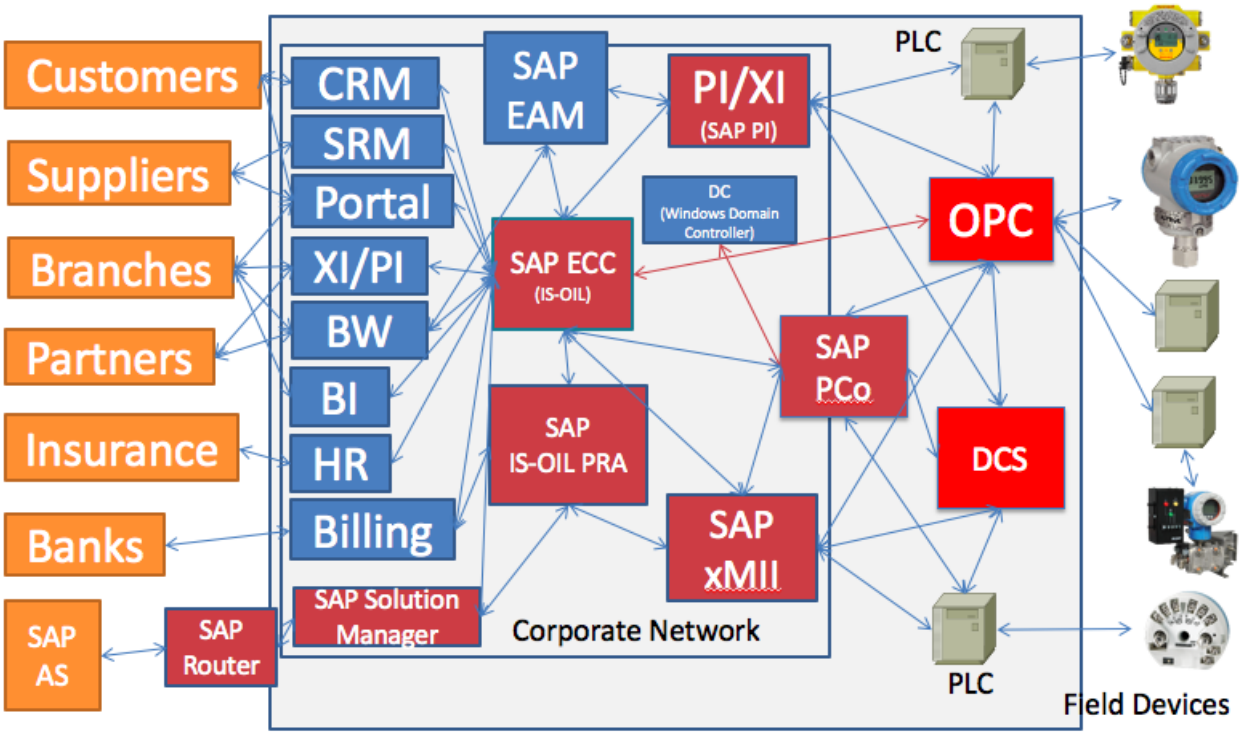
  - SAP EAM (+AssetWise APM), Oracle EAM (Based on EBS), Schneider Electric's Avantis EAM, IBM Maximo
  - Connect with: OSIsoft® PI System, AspenTech® IP21, Honeywell® PHD

- LIMS <- Refinery
  - Custom app based on Oracle DBMS

- Tank Master Data (TMD) <- Tank Inventory

  - SAP IS-OIL-TAS, Aspentech
- Production Accounting System (PAS) <- Fiscal Metering
  - SAP IS-OIL-PRA

In real life a simple scheme may look like this:



Attacking Oil and Gas

From the Internet to CORP

There are many ways how an attacker can get access to the corporate network. Here are some of the most common options. You can find more examples in out previous SAP Security presentations

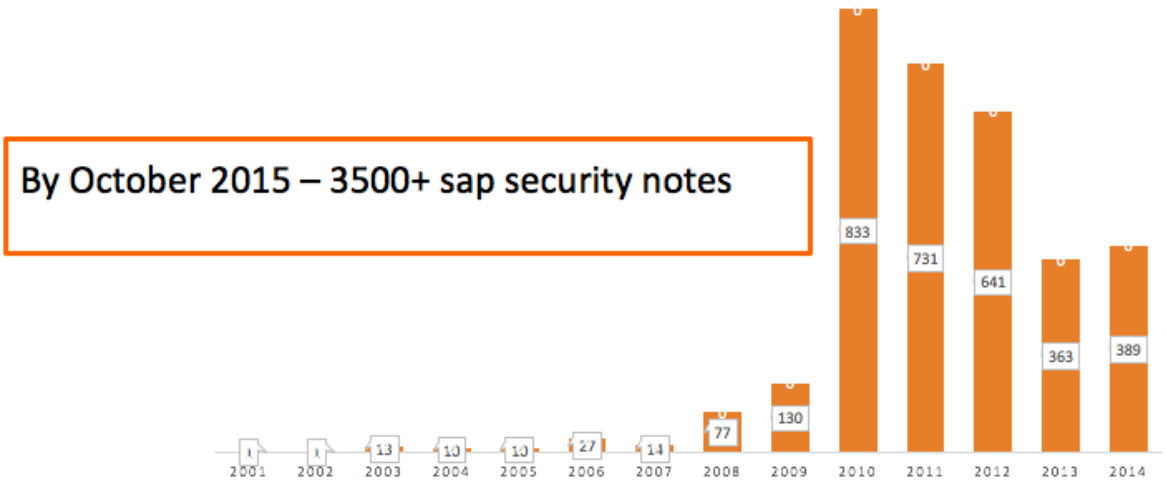
- Via Internet resources (SAP Portal/CRM/SRM)
  - http://erpscan.com/wp-content/uploads/2013/07/SAP-Portal-Hacking-and-Forensics-at-Confidence-2013.pdf
- Via Partners (SAP XI)
  - http://erpscan.com/wp-content/uploads/publications/SSRF-vs-Businness-critical-applications-final-edit.pdf
- Via SAP Router
  - http://erpscan.com/advisories/dsecrg-13-013-saprouter-heap-overflow/
- Via Workstations (Trojans)
  - http://erpscan.com/wp-content/uploads/publications/SAP-Security-Attacking-SAP-clients.pdf
- Via Unnecessary SAP Services exposed to the Internet
  - http://erpscan.com/wp-content/uploads/publications/SAP-Security-Attacking-SAP-clients.pdf

From Internal (CORP) Network to ERP

There a numerous ways how an ERP system can be compromised:

- Vulnerabilities
- Misconfigurations
- Unnecessary privileges
- Custom code issues

Vulnerabilities



Misconfigurations

Enterprise applications are very complex, and as you may know, complexity kills security. For example, only in SAP systems you can find:

- ~1500 profile parameters
- ~1200 web applications
- ~700 web services
- ~100 specific commands for MMC
- ~100 specific checks for each of the 50 modules (FI, HR, Portal, MM, CRM, SRM, PLM, Industry solution…)

All these configurations can be improperly implemented thus allowing cybercriminals to obtain access to mission-critical systems. You can find some SAP Security guides on our website

Custom code issues

Domain specific languages in business applications (ABAP, Peoplecode, XSJS, X++) can have vulnerabilities as well as backdoors left by 3rd party developers. You can find which code vulnerabilities are most common in custom SAP Applications. [16]

Unnecessary privileges

Critical privileges and SoD issues

- For example: one can create a fake vendor and then approve payment order for this vendor.
- Usually ((~100 Roles X 10 actions)^2)/2=500k
- 500k potential conflicts for each user!
- Usually, it takes two years to decrease the number of conflicts from millions to hundreds.
- And you still will be vulnerable

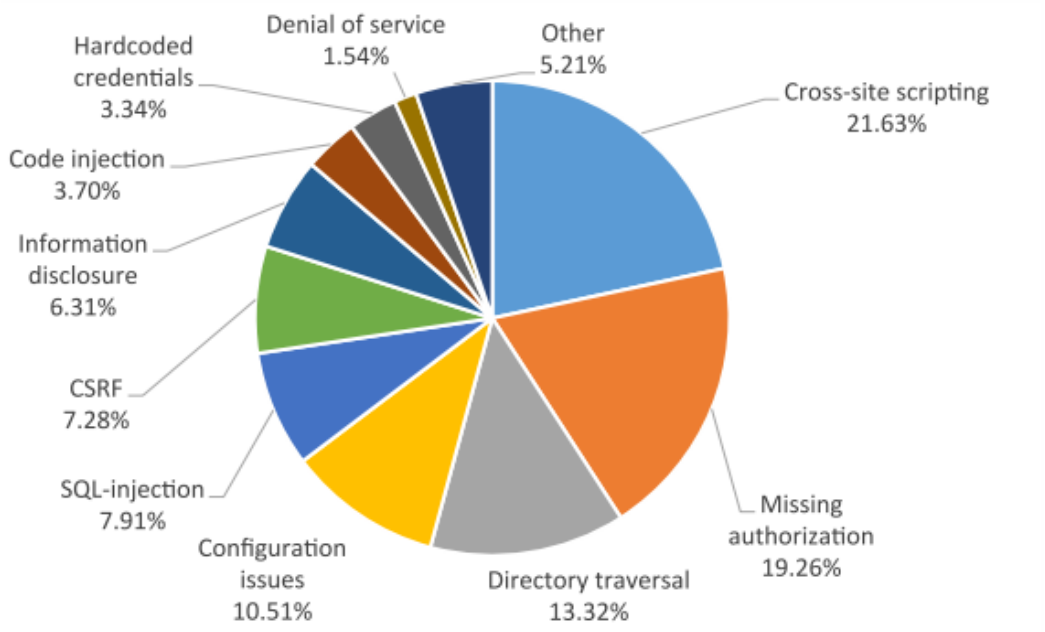


Figure 3.4-1 TOP-10 SAP Security Vulnerabilites, sorted by type

From ERP to OT

Now we have the final stage, how to pivot from business applications to critical processes. Usually, there are following links between them. Please keep in mind that it is just the tip of the iceberg.

- **SAP ERP -> SAP XMII -> SAP PCo -> DCS/SCADA -> PLC -> Meter**
- SAP ERP -> SAP XMII -> SAP PCo -> PLC -> Meter
- **SAP ERP -> SAP XMII -> DCS/SCADA(OPC) ->PLC-> Meter**
- SAP ERP -> SAP PCo -> OPC Server -> PLC -> Meter
- SAP ERP -> SAP PCo -> PLC -> Meter
- SAP ERP(PP) -> SAP PI -> OPC-> PLC -> Meter
- SAP ERP(PP) -> SAP PI -> SAP xMII->OPC -> PLC -> Meter
- SAP PM (EAM) -> OsiSoft PI -> OPC
- **SAP HANA(Rolta OneView) -> OPC/DCS ->PLC->Meter**
- Oracle DB (LIMS) -> DCS -> PLC-> Meter
- **Domain Controller -> SAP PCo -> PLC -> Meter**
- Shared SSH keys
- Similar passwords
- Improper firewall configurations

ERP entry point

HANA

There are several possible paths to get a handle on the industrial processes. SAP HANA is an in-memory database solution that combines database, application processing, and integration services on a single platform.

It is a good candidate to store data about industrial processes and render them in real-time. SAP HANA had several critical vulnerabilities and at the end of September we reported a unthenticated remote code execution vulnerability via a memory corruption bug. It is the perfect way to get an entrance ticket to the OPC servers that are directly connected to HANA.

SAP Manufacturing Integration and Intelligence

There are more common ways of interconnecting the ERP world to the industrial one. The prevalent architecture uses the SAP MII solution to collect industrial data from SAP Plant Connectivity (PCo) that relays information sent from OPC server or DCS/SCADA systems.

MII stands for Manufacturing Integration and Intelligence. SAP MII provides a direct connection between shop-floor systems and business operations.

SAP MII is a technology following the SAP xApps convention and running on a SAP NetWeaver application server. SAP xApps are composite applications which can combine web services and data from multiple systems. The application architecture is defined by the SAP Composite Application Framework within the SAP NetWeaver platform. The framework includes the methodology, tools, and run-time environment to develop composite appliations. It provides a consistent object model and allows developers to build composite applications with a rich user interface, which can access multiple other heterogeneous applications via services.

From an attacker's point of view, it is a fertile ground for interesting vulnerabilities.

From a technical perspective, MII is accessed through its main application `xmii~xapps~ears` and serving several servlets at different URL endpoints defined in a web.xml file. The web entry point is defined as 'XMII'. It means that if our server (by default) listens to the TCP port 50000, we should have access to its MII part at the URL http://server:50000/XMII.

Getting admin rights on the Netweaver platform

SAP Netweaver stores its persistent data in a Sybase database. We can locate the tables where the users encrypted credentials are stored, but how to get them?

By analyzing several servlets (non-MII related), we found several vulnerabilities and especially a

blind SQL injection that allows to read the content of SYSTEM tables anonymously and those owned by our MII application under certain conditions.

With a time-based comparison between successful SQL requests and failing ones, we can get one character per request the content of the hashed password of the Administrator. Another weakness in the way the password is encrypted get us the clear text password.

While those problems are still being dealt by SAP, we can't disclose any details.

Getting OS rights on the MII server

After getting those Administrator credentials, we can profit with the rich user experience provided by the web admin interface. We, for instance, found out that through the "Log viewer" feature we can ask the server to connect to a remote system on port 50013 with the protocol "SAP Instance Agent".

This functionality uses the SAPControl web services accessible via a SOAP web interface on TCP port 50013 to get information about server health. This service is offered by the daemon sapstartsrv that is the parent of all the other SAP instances. It exposes a vast number of methods, as some of them have several vulnerabilities like information disclosure and remote command execution in the past.

SAP Technical Documentation says about it: *« The SAP Start Service (sapstartsrv) provides basic management services for systems and instances and single server processes. Services include starting and stopping, monitoring the current run - time state, reading logs, traces and configuration files, executing commands and retrieving other technology - specific information, like network access points, active sessions, thread list etc. They are exposed by an SOAP Web service interface named "SAPControl" »*

Of course, the last part mentioning "executing command" will hold our attention.

Usually, the authentication methods of this SOAP service should be used with an OS level user account (miiadm in this case), but there are some undocumented features...
If we open the port 50013 on our computer we will see something like :

```
POST /SAPHostControl.cgi HTTP/1.1
Host: 172.16.2.31:50013
Content-Type: text/xml; charset=UTF-8
Connection: close
Authorization: Basic ezI[...]eA==
SAP-PASSPORT: 2A54482A0300E600[...]
Content-Length: 334
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8" ?><SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema"><SOAP-
ENV:Body><yq1:GetVersionInfo
xmlns:yq1='urn:SAPControl'></yq1:GetVersionInfo></SOAP-
ENV:Body></SOAP-ENV:Envelope>
```

When analyzing the reverse connection made by the server to our computer, we notice it uses the HTTP header "Authorization" with credentials base64 encoded and sends a SOAP request, assuming that we will have an SAP Control speaking service at our end. The server leaks us its internal trusted account password (this password is random and changes every time the service is started).

If we use the SOAP method OSExecute() with this special account, we get a remote command execution with 'miiadm' rights. With a custom SOAP python wrapper we can easily consume this service like this:

```
$ soap_cli.py --host $SAPMII --port 50013 \
              --user [redacted] --password [redacted] \
           --method OSExecute /usr/bin/whoami
(200, (reply){
   exitcode = 0
   pid = 29342
   lines =
      (ArrayOfString){
         item[] =
            "miiadm",
      }
 })
```

It doesn't take to long to have an interactive shell with 'miiadm' user rights (without knowing its password).

Even if this is not necessary to reach our goal, we can then read the Netweaver SecretStore files (properties and key) to decrypt different accounts and passwords of the Sybase database because they are readable by the miiadm user.

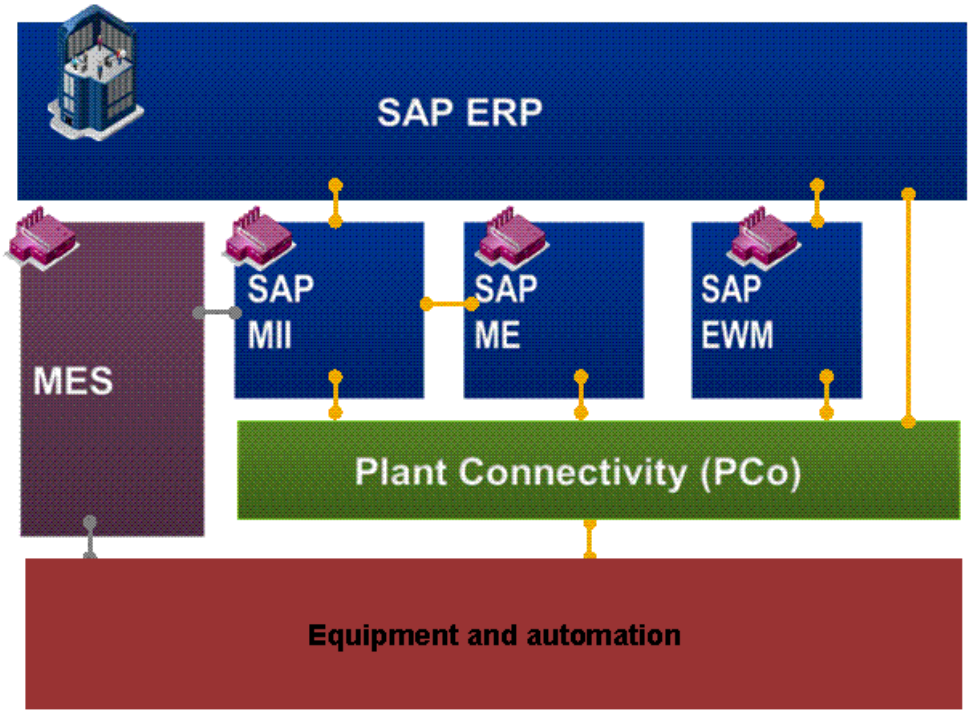
Another attack vector to get OS access on MII is to use a directory traversal vulnerability and a file disclosure to get the SecStore files, access Sybase with administrative rights and use the external procedure `xp_cmdshell` if available.

SAP Plant Connectivity

SAP MII can get its industrial data through SAP Plant Connectivity also named PCo. It acts like a bridge between the industrial world and the ERP one. It enables to define agents that send some tags from sources to a destination (like in this case SAP MII) with a built-in decision engine.

The sources are, for instance, Matrikon OPC Server, Siemens Simatic or KEPServerEX, for the well-used OPC implementations.

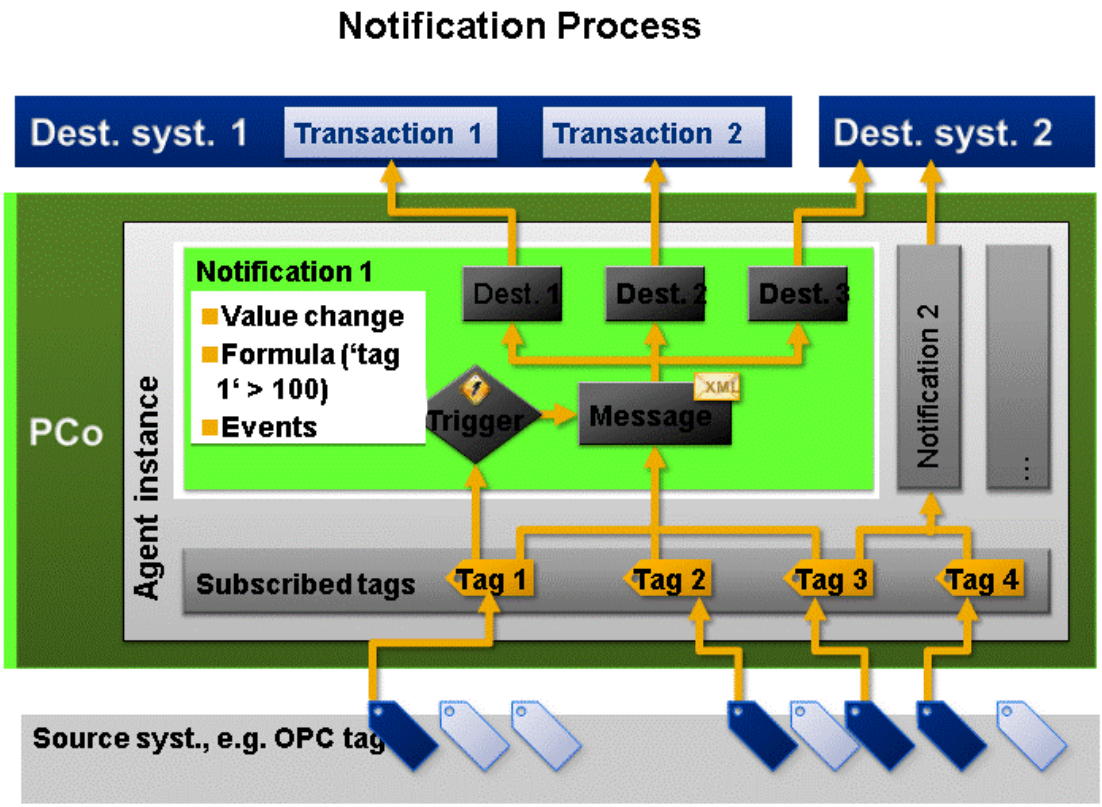
Integration of Plant Connectivity in the System Landscape



The setup between SAP MII and SAP PCo can follow two main modes:

- Notification mode
- Query mode

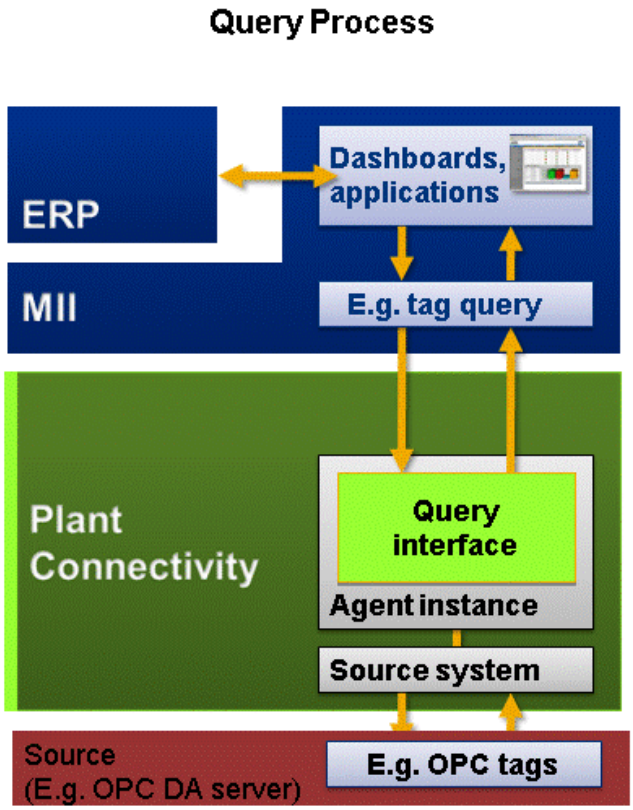
In case of the notification process, PCo sends its data to MII "Transactions" via a web service endpoint and transmitting user credentials via HTTP Basic Authentication. The connection can be secured using SSL and there is a check box to allow connections with untrusted server certificate. By default, the connection is done via HTTP.



As for an attacker sitting on MII, this connection mode doesn't give a lot about PCo. Let's have a look at the Query mode.

This mode allows MII to send queries to PCo and retrieve operational data. It uses a custom SAP protocol designed over XML named xMII. The basics are to retrieve data and store data. PCo will forward those requests to its sources that deliver the data.

In SAP MII, to enable this mode we need to add a new Data server with a connector type PCoConnector. Then we need to fill either a URL to the PCo instance or to get registered our PCo instance from the SLD (System Landscape Directory). The URL corresponding to the Management SOAP service looks like this: http://pcoserver:50050/PCoManagement. We will come back to that soon.



The test connection that is made to the SOAP service requires valid Windows credentials. We notice the agent port (default to tcp/9000) that is retrieved from the configuration. It is through this port that will be exchanged the special xMII packets.

Our question now is where and in what form those credentials are stored. We found out that the `SAPSR3DB.XMII_SERVERPROP` contains all the data about data servers and the password is encrypted with 3DES with the key being stored inside the SecureStorage service. The SecureStorage is used like a vault, and each application gets a specific handle to access its own private data.

The idea was to connect from the outside with our stolen NetWeaver admin credentials via ICM, connect to the service and dump the key associated to our XMII application, but it failed. The access to SecureStorage is denied if it doesn't come from a trusted execution path. There is a call stack validation enforced.

We didn't get too far about circumventing that with modifying the XMII application (we still can deploy code with admin rights) when we found that we can just lower the encryption scheme to Base64. It then become trivial to SQLi the correct database column and return the clear text password of our Windows PCo user.

We then can fully control the PCo behavior from its SOAP authenticated endpoints - start, stop agent, get information about sources, dump configuration, load a different configuration.

That is interesting, of course, but what about modifying the live data or fake them? That's where

the query port tcp/9000 comes into play. By default, the communication is not authenticated. We can send our own requests from our MII access and they will be forwarded to the industrial sources.

Disclosing data from industrial process (learning)

After having identified several (undisclosed) problems with the implementation of the server on PCo, we can read the exported tags of the OPC server for all the running agents with our own xMII client. It means raw industrial data from the shop-floor.

The xMII requests are encapsulated in an XML message with the tag operations being sent as CDATA. Asking, for instance, the value of the water level in our setup system based on a S7-1200 will look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
    <pco:request xmlns:pco="uri:sap-pco-request"
pco:version="1.0">
        <pco:tag>
            <![CDATA[RETRIEVE 'TCPIP>S7>IW66';]]>
       </pco:tag>
    </pco:request>
```

Where the tag `TCPIP>S6>IW66` has been defined to be an alias for the S7 memory value at address `%IW66`. We can make the following parallel with files and directories in a regular filesystem with the groups and tags from an OPC server. It means that if we want to know the base directories we will send the request containing the following CDATA `'LIST GROUPS'`. If we want to list the tags in a specific group, we send `'LIST TAGS IN "$GROUP"` with `$GROUP` being replaced with the value received in the group list request. We can list recursively all the tags available with one command `'LIST TAGS RECURSIVELY'`.

Modifying data

If there are exported tags with default read-write rights, then we can use the `STORE` command to change their value. That can be disastrous in some case, of course…
We can use that in our setup to activate the water tap of our tank. The tag for the tap is at address `%M1.0` where a boolean is accessible with read and write access.

```
<?xml version="1.0" encoding="UTF-8"?>
    <pco:request xmlns:pco="uri:sap-pco-request"
pco:version="1.0">
        <pco:tag>
            <![CDATA[STORE 'TCPIP>S7>M1.0' = 1;]]>
        </pco:tag>
```

```
    </pco:request>
```

We just opened the tap, and the water is flowing out of the tank now. We can monitor the water level with the previous read command to memory`%IW66` and when everything is done, we close the tap with the similar operation, writing the «`False`» value to the memory address of the tap's tag.

```
<?xml version="1.0" encoding="UTF-8"?>
    <pco:request xmlns:pco="uri:sap-pco-request"
pco:version="1.0">
        <pco:tag>
            <![CDATA[STORE 'TCPIP>S7>M1.0' = 0;]]>
        </pco:tag>
    </pco:request>
```

Faking data

With this knowledge, we can build our own PCo server answering to the usual MII requests with previously learned values while in the background disrupting the industrial process. We can control agents states on the real PCo instance. The data server in MII configuration has just to be pointed to our (local) service hosted on MII.

Conclusion

The report has demonstrated that it is possible to perform three attack vectors, and, most importantly, to penetrate into business critical processes, which allows an attacker to carry out further attacks.
Apart from risks directly related to ICS systems, there are some other threats that might look less critical but in the worst scenario they can cost companies millions and even disrupt whole business.
Even there aren't any vulnerabilities in components of industrial systems, insecure configurations and not updated business applications may put a company at the following risks:

Plant equipment sabotage

Hackers can fake data about temperature, pressure and other conditions. For example, they can spoof a report about a problem with equipment in a remote facility. Companies will spend a lot of time and money to investigate the incident if this facility is situated somewhere in the middle of the ocean. This can be done by exploiting vulnerabilities described in our report. The easiest way to do so is to hack an asset management solution.

Company Sabotage

Hackers can send fake information about oil quantity to managers who make their decisions based on this data.
Assume that every day one sends information that there is much more oil in stock that we really have. The company will sell out all the oil and won't be able to deliver it to customers. The failure to perform the obligations could lead to a global scandal, changes in oil prices and huge losses up to the company's bankruptcy.
Some of the tank information management solutions feature commands to PLC devices to change values such as the maximum filling limit of tanks. In that case, hackers can send those commands and perform a successful attack that may lead to oil explosion.

Plant Destruction

BMS Systems and some other critical systems are used in numerous processes including Separation и Refinery. Some of the critical systems not only send information, but also allow you to manage them through third-party systems, such as ERP, EAS, LIMS remotely via intermediate systems SAP PCo and SAP MII, and some of the solutions allow sending particular commands to PLC from ERP/MES system. PCo provides a framework to create custom agents which can be used to send commands to PLC. This is one of the ways how to attack ICS even there are no vulnerabilities in PLC/SCADA/DCS systems

Any vulnerabilities in industrial systems can be exploited if one has an access to the industrial network because of insecure separation between IT and OT networks. Then a company will face all the risks listed at the beginning of the document:

Plant Sabotage/Shutdown
Equipment damage
Utilities Interruption
Production Disruption (stop or pause manufacturing process)
Product Quality (bad oil and Gas quality)
Undetected Spills
Illegal taping
Compliance violation (pollution)
Safety violation (death or injury)

References

1. Hackers' Favorite Target: Big Oil and All That Deadly Equipment http://www.bloomberg.com/news/articles/2015-06-10/hackers-favorite-target-big-oil
2. The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systemshttps://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems-wp.pdf
3. Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised http://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised
4. Internet attack could shut down US gas stations http://arstechnica.com/security/2015/01/internet-attack-could-shut-down-us-gasoline-stations/
5. Oil and Gas Production Handbook http://www.saudienergy.net/PDF/Intro%20Oil.pdf
6. Data Sheet “Net Oil & Gas Solution” http://iom.invensys.com/EN/pdfLibrary/Datasheet_Foxboro_Net%20Oil%20and%20Gas%20Solution_10-13.pdf
7. Burner Management System Solutions http://iom.invensys.com/EN/pdfLibrary/Brochure_Triconex_BurnerManagementSystemSolutions_08-10.pdf
8. Burner Management Systems http://www2.emersonprocess.com/en-us/brands/deltav/sis/applications/pages/bms.aspx
9. Burner Management System SIMATIC BMS400F http://www.industry.usa.siemens.com/topics/us/en/bms/bmsinformation/Documents/BMSBrochureAPPROVED.pdf
10. Burner Management System (BMS) - Safety Solution for the Power Generation Industry https://www.honeywellprocess.com/en-US/explore/products/control-monitoring-and-safety-systems/safety-systems/Pages/burner-management-system.aspx
11. Custody transfer https://en.wikipedia.org/wiki/Custody_transfer
12. Oil and Gas Custody Transfer http://www2.emersonprocess.com/siteadmincenter/PM%20Articles/Oil-and-Gas-Custody-Transfer_petroleum_africa_may_2014.pdf
13. Best Practices for DanPac Express Cyber Security http://www2.emersonprocess.com/siteadmincenter/PM%20Daniel%20Documents/Whitepaper_DanPac%20Express%20Cyber%20Security%20Best%20Practices.pdf
14. FloBoss S600+ Flow Computer http://www.documentation.emersonprocess.com/groups/public/documents/specification_sheets/d301151x012.pdf
15. Oil refinery https://en.wikipedia.org/wiki/Oil_refinery
16. Analysis of 300 vulnerabilities in SAP http://erpscan.com/wp-content/uploads/publications/3000-SAP-notes-Analysis-by-ERPScan.pdf

Additional reading

- The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems https://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems-wp.pdf

- Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion.pdf

- http://blackhat.com/docs/us-14/materials/us-14-Larsen-Miniturization.pdf

- Physical Damage 101: Bread and Butter Attacks https://www.blackhat.com/docs/us-15/materials/us-15-Larsen-Remote-Physical-Damage-101-Bread-And-Butter-Attacks.pdf

About ERPScan

ERPScan is the most respected and credible Business Application Security provider. Founded in 2010, the company operates globally. Named as an 'Emerging vendor' in Security by CRN and distinguished by more than 30 other awards - ERPScan is the leading SAP SE partner in discovering and resolving security vulnerabilities. ERPScan consultants work with SAP SE in Walldorf supporting in improving security of their latest solutions.

ERPScan's primary mission is to close the gap between technical and business security, and provide solutions to evaluate and secure ERP systems and business-critical applications from both, cyber-attacks as well as internal fraud. Usually our clients are large enterprises, Fortune 2000 companies and managed service providers whose requirements are to actively monitor and manage security of vast SAP landscapes on a global scale.

Our flagship product is ERPScan Security Monitoring Suite for SAP. This multi award-winning innovative software is the only solution in the market certified by SAP SE covering all tiers of SAP security i.e. vulnerability assessment, source code review and Segregation of Duties. The largest companies from across diverse industries like oil and gas, banking, retail, even nuclear power installations as well as consulting companies have successfully deployed the software. ERPScan Monitoring Suite for SAP is specifically designed for enterprise systems to continuously monitor changes in multiple SAP systems. It generates and analyzes trends on user friendly dashboards, manages risks, tasks and can export results to external systems. These features enable central management of SAP system security with minimal time and effort.

We use 'follow the sun' principle and function in two hubs, located in the Netherlands and the US to operate local offices and partner network spanning 20+ countries around the globe. This enables monitoring cyber threats in real time while providing an agile customer support.

About ERPScan Research Team

The company's expertise is based on the research subdivision of ERPScan, which is engaged in vulnerability research and analysis of critical enterprise applications. It has achieved multiple acknowledgments from the largest software vendors like SAP, Oracle, Microsoft, IBM, VMware, HP for exposing in excess of 400 vulnerabilities in their solutions (200 of them just in SAP!).

ERPScan researchers are proudly to expose new types of vulnerabilities (TOP 10 Web hacking techniques 2012) and were nominated for best server-side vulnerability in BlackHat 2013.

ERPScan experts have been invited to speak, present and train at 60+ prime international security conferences in 25+ countries across the continents. These include BlackHat, RSA, HITB as well as private trainings for SAP in several Fortune 2000 companies.

ERPScan researchers lead project EAS-SEC, which is focused on enterprise application security research and awareness. They have published 3 exhaustive annual award-winning surveys about SAP Security.

ERPScan experts have been interviewed by leading media resources and specialized info-sec publications worldwide, these include Reuters, Yahoo, SC Magazine, The Register, CIO, PC World, DarkReading, Heise and Chinabyte to name a few.

We have highly qualified experts in staff with experience in many different fields of security, from web applications and mobile/embedded to reverse engineering and ICS/SCADA systems, accumulating their experience to conduct research in SAP system security.

Our Contacts

Global Headquarters: 228 Hamilton Avenue, Fl. 3, Palo Alto, CA. 94301

Phone: 650.798.5255

EMEA Headquarters: Luna ArenA 238 Herikerbergweg, 1101 CM Amsterdam

Phone: +31 20 8932892

Twitter: @erpscan

Web: www.erpscan.com

Contact: info@erpscan.com

PR: press@erpscan.com