

Invest in security to secure investments



# SAP Cybersecurity for Oil and Gas



Alexander Polyakov - CTO, ERPScan

Mathieu Geli - Head of SAP Threat Intelligence, ERPScan

- The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP and Oracle
- **Leader** by the number of **acknowledgements from SAP** ( 150+ ) and Oracle (40+)
- **60+ presentations** key security conferences worldwide
- **30+ Awards and nominations**
- Research team – **20+ experts with experience in different areas of security from ERP to ICS and Mobile**
- Headquarters in Palo Alto (US) and Amsterdam (EU)

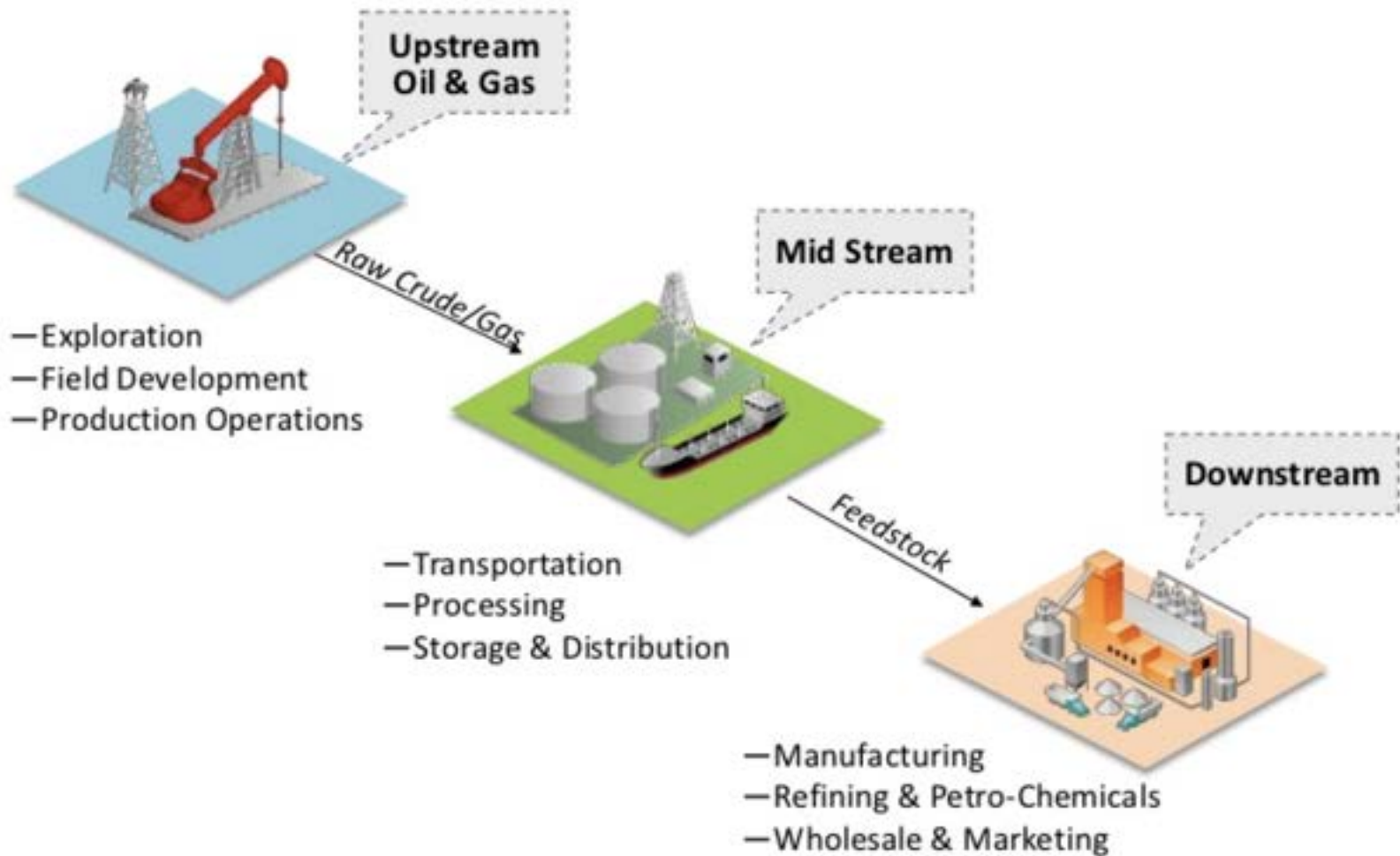


- ERPScan and SAP
  - Researching since 2007
  - 200+ vulnerabilities found
  - Applications covered: ERP, CRM, SRM, Business Objects, SAP GUI, HANA, Mobile, NetWeaver J2EE, Portal, SDM
- ERPScan and Oracle
  - Researching since 2008
  - 40+ vulnerabilities, 16 times acknowledged in Oracle CPU
  - Applications covered: Oracle DB, Oracle EBS, Oracle BI, Oracle PeopleSoft, Oracle JDE

- This is NOT a traditional type of talk
- For me neither
- There are more questions than answers
- There is the first technical Oil and Gas Cybersecurity talk
- This is just a beginning

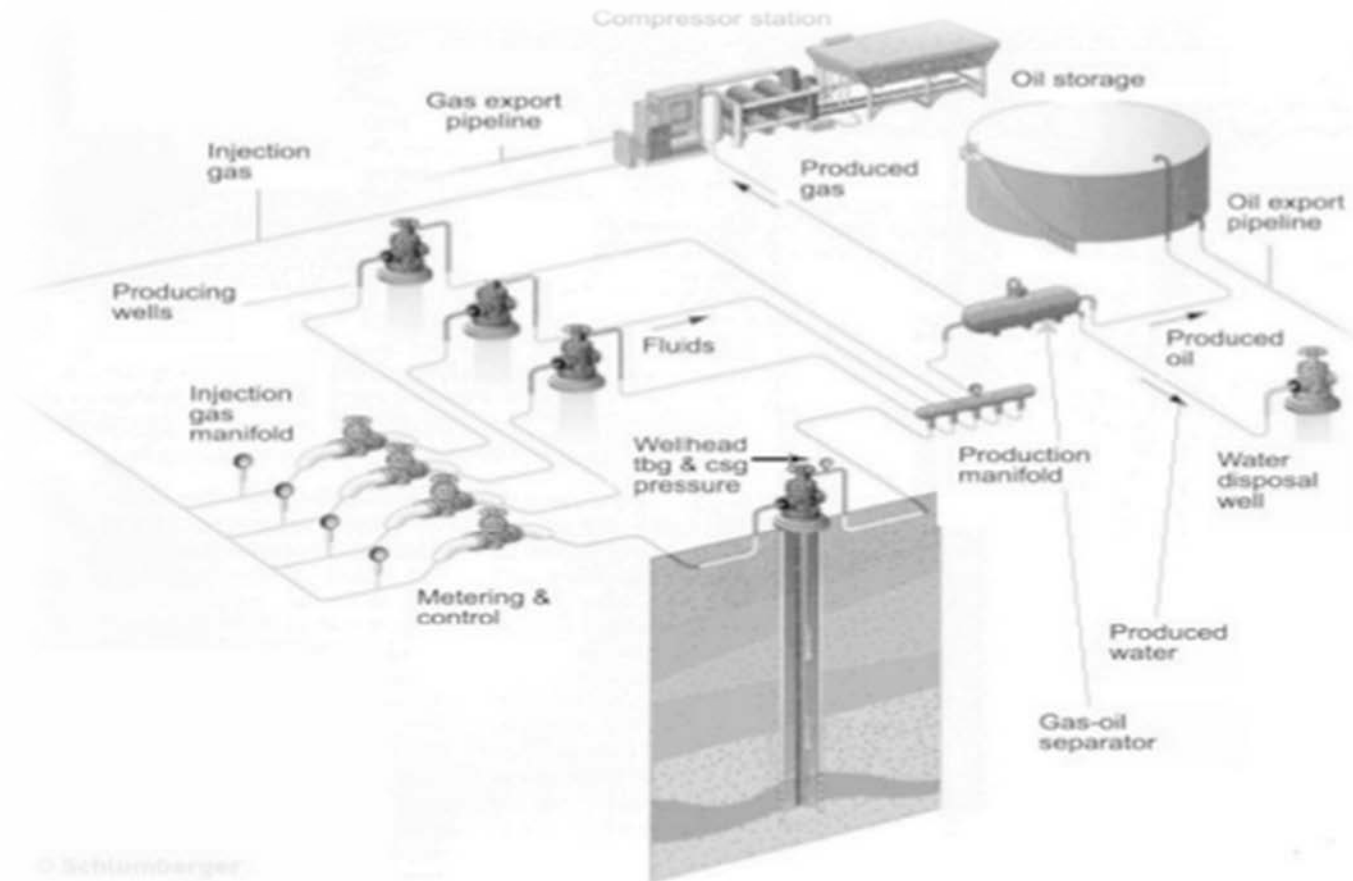
The oil and gas industry is usually divided into three major sectors

- **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.





# Typical Upstream processes (Onshore)



Simple Upstream oil and gas process

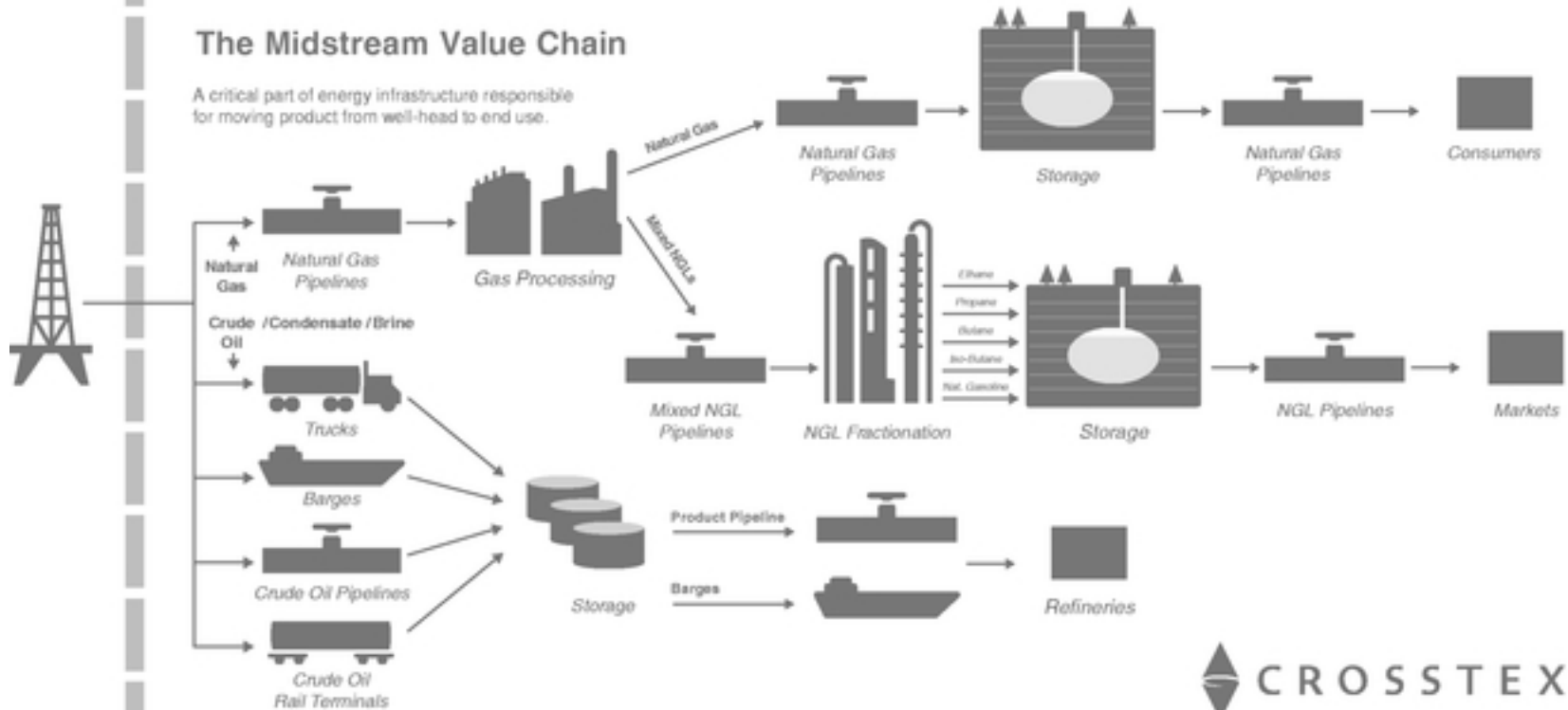
- Extraction (Drilling)
  - Pump controllers, blowout preventers, Flaring and Venting
- Gathering (From earth to separators)
  - Wellhead management, Manifolds management, net oil measurement
- **Separation (Separate oil, gas and water)**
  - Multiple separators (2phase/3phase), Heaters, **Burners**, Coalescence, Desalting
- Gas compression (Prepare for storage and transport)
  - Multiple stages
- Temporary Oil Storage (Temporarily store before loading)
- 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





## The Midstream Value Chain

A critical part of energy infrastructure responsible for moving product from well-head to end use.



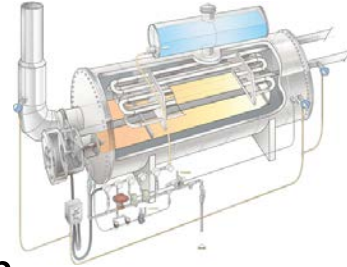
- Terminal management (Obtain oil from upstream)
  - Measurement, Automation, Order Movement Management
- Gas Processing (Separate natural gas and NGL)
- Gas Transportation (transfer gas to storage)
  - Pipeline management
- Oil transportation (transfer oil to storage)
  - Pipeline management
- Gas storage (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

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

**Plant Sabotage/Shutdown**  
**Equipment damage**  
**Utilities Interruption**  
**Production Disruption (Stop or pause production)**  
**Product Quality (bad oil and gas quality)**  
**Undetected Spills**  
**Illegal pipeline taping**  
**Compliance violation (Pollution)**  
**Safety violation (Death or injury)**

## Some critical processes in Oil and Gas: details

- Gas Oil Separation Plant
- Risks:
  - Product Quality, Equipment damage
- Management systems
  - ABB Totalflow XFC
  - Yokogawa CENTUM CS 3000
- Burner Management Systems (BMS)
- Compressor Control System (CCS)
- Vibration Monitoring System (VMS)



- Risks:
  - Product Quality, Equipment damage
  - Plant Sabotage, Production Disruption, Compliance violation
- Used in a variety of applications:
  - **Separators**, tanks, heaters, Incinerators, Flare stacks, etc.
- Management systems:
  - **Emerson's DeltaV SIS**, Invensys BMS, Honeywell's BMS, Combustex BMS-2000, Allen-Bradley, Siemens SIMATIC BMS400F
- PLC vendors:
  - GE, Modicon, Allen-Bradley, Koyo, Siemens
- Flame sensors:
  - Fireye, PPC, Honeywell, IRIS, Coen

- Risks:
  - Product Quality, Monetary loss
- Analyzes density, viscosity of water content, temperature, and pressure
- Divided into several runs
- Each run employs one meter and several instruments for temperature and pressure correction
- Gas metering is less accurate (+-1%)
- LNG metered within mass flow meters





## How Custody Transfer Works

- Custody transfer, sometimes called fiscal metering, occurs when fluids or gases are exchanged between parties.
- Payment is usually made as a function of the amount of fluid or gas transferred.
- 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 of oil per minute. A small error of 0.1% equates to about \$100,000 a day. Over a year, the 0.1% error would amount to a difference of \$50m.
- 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.

**Error levels that would be tolerable in a process plant context can cost one side or the other tens of thousands of dollars in a matter of hours.**

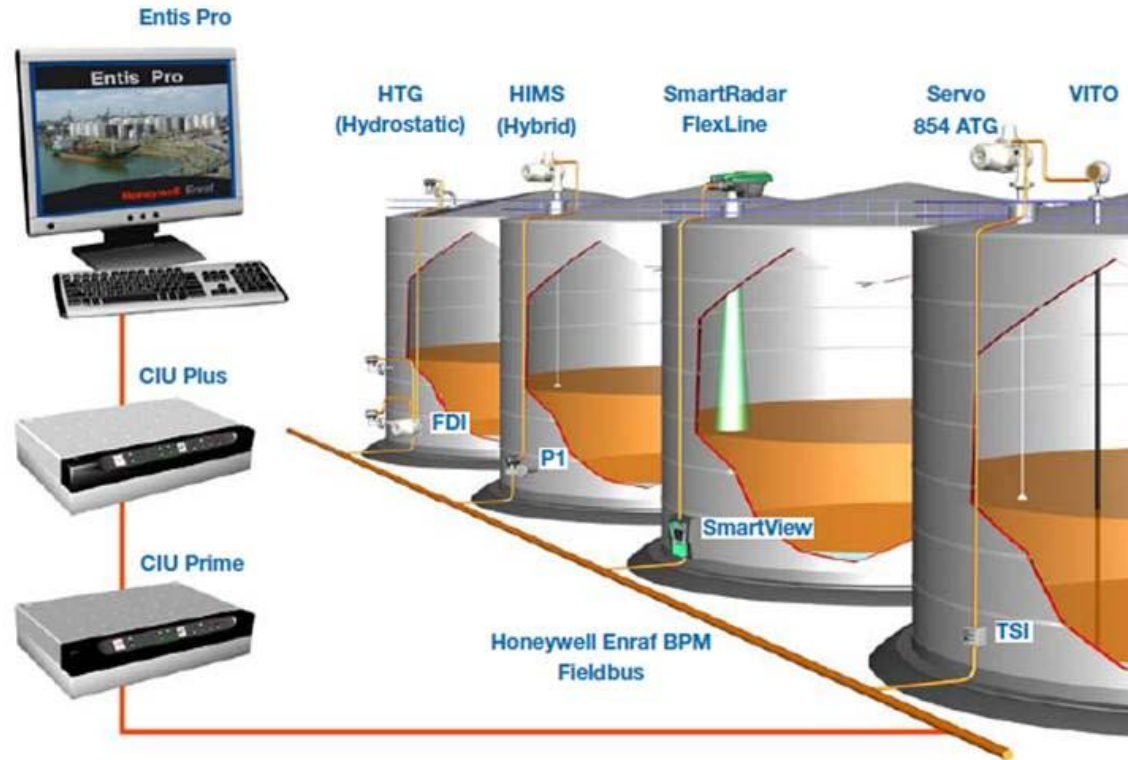
- Production Accounting System
- Data Aggregation and management (easy to manipulate)
  - FlawCall – FlawCall Enterprise (! Internet access)
  - **KROHNE SynEnergy** (! Internet access + SAP access)
  - Honeywell's Experion® Process Knowledge System (PKS), MeterSuite™
  - OPC Servers (Keepware, MatrikonOPC) (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.

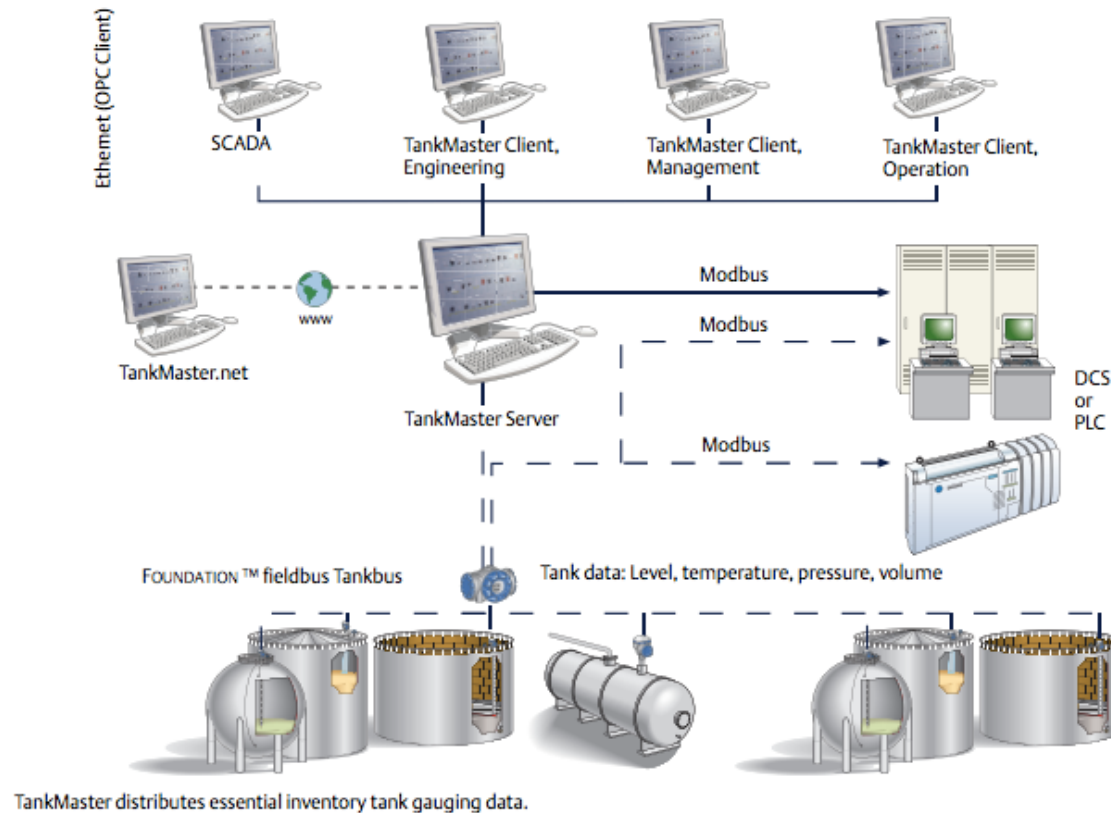


- Risks
  - Plant Sabotage/Shutdown, Equipment damage, Production Disruption, Compliance violation, Safety violation
- Tank Inventory System collects data from special tank gauging systems such as level radars, pressure or float that are used to measure the level in storage tanks
- Can usually consist of 10-100+ tanks with 1-50m barrels
- Accurate records of volumes and history are kept
- **Forecasting for stock control**

- Monitoring the levels in offsite storage tanks of flammable materials in particular can significantly reduce the likelihood of initiating events that could have a potential impact not only on operation but also on safety and the environment.
- Tank level deviations can result in hazardous events such as a tank overfilling, liquefied gas flashing etc.
- 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.

- Connection with IT
  - Enraf TM BOX
  - Honeywell's Experion® Process Knowledge System (PKS) (For Terminals)
- Tank Inventory Systems (single-window interface to operate 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





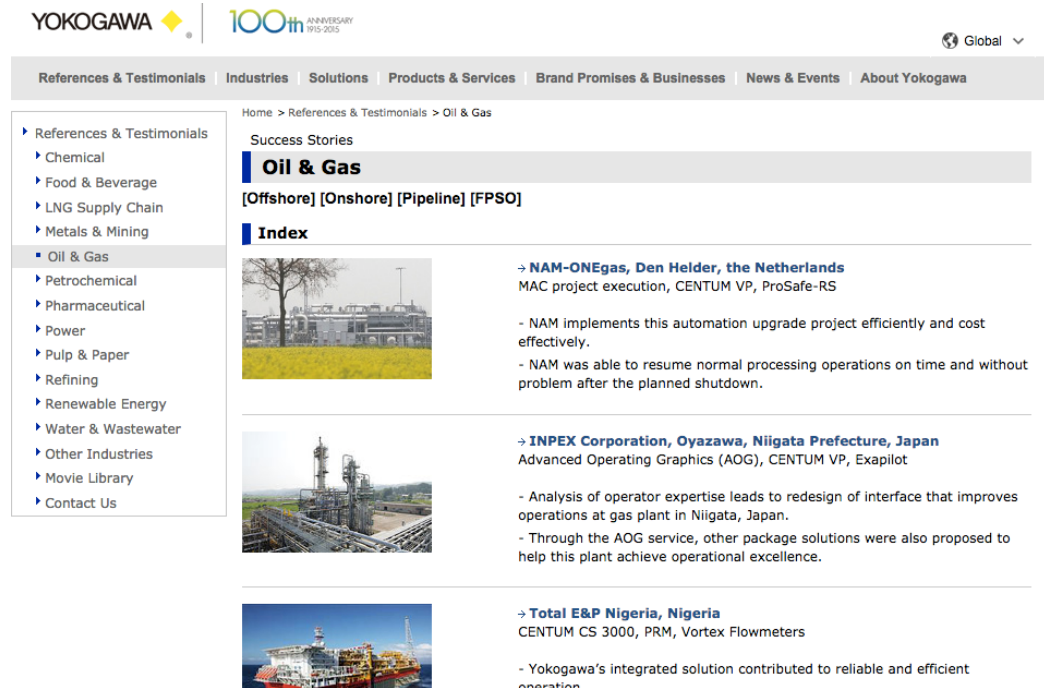
- Management console Emerson Rosemount TankMaster WinOpi
- View and **control!**
- Control commands
  - Changing any alarm (Level, Temperature, Pressure)
  - For tanks configured as servo tanks, it is possible to send commands to a servo gauge, such as an Enraf
    - Freeze, Lock



- 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 more useful products such as 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 much of the technology of, and can be thought of, as types of chemical plants.

- Corp net connection
  - Emerson DeltaV, OSIsoft PI
- Management
  - 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

- Press releases
- Vendor success stories
- LinkedIn
- StackOwerflow
- TechTarget
- etc.



The screenshot shows the Yokogawa website's 'References & Testimonials' section, specifically the 'Oil & Gas' category. The page features a navigation menu on the left with categories like Chemical, Food & Beverage, LNG Supply Chain, Metals & Mining, Oil & Gas (selected), Petrochemical, Pharmaceutical, Power, Pulp & Paper, Refining, Renewable Energy, Water & Wastewater, Other Industries, Movie Library, and Contact Us. The main content area displays 'Success Stories' for 'Oil & Gas', with sub-sections for '[Offshore]', '[Onshore]', '[Pipeline]', and '[FPSO]'. Three success stories are listed, each with a thumbnail image and a brief description of the project and the solutions implemented.

**YOKOGAWA** | 100th ANNIVERSARY 1915-2015

Global

References & Testimonials | Industries | Solutions | Products & Services | Brand Promises & Businesses | News & Events | About Yokogawa

Home > References & Testimonials > Oil & Gas

**Success Stories**

**Oil & Gas**

[Offshore] [Onshore] [Pipeline] [FPSO]

**Index**

→ **NAM-ONEgas, Den Helder, the Netherlands**  
MAC project execution, CENTUM VP, ProSafe-RS

- NAM implements this automation upgrade project efficiently and cost effectively.
- NAM was able to resume normal processing operations on time and without problem after the planned shutdown.

→ **INPEX Corporation, Oyazawa, Niigata Prefecture, Japan**  
Advanced Operating Graphics (AOG), CENTUM VP, Exapilot

- Analysis of operator expertise leads to redesign of interface that improves operations at gas plant in Niigata, Japan.
- Through the AOG service, other package solutions were also proposed to help this plant achieve operational excellence.

→ **Total E&P Nigeria, Nigeria**  
CENTUM CS 3000, PRM, Vortex Flowmeters

- Yokogawa's integrated solution contributed to reliable and efficient operation

## Enterprise Applications in Oil and Gas

## SAP (ABAP, J2EE Mobile, HANA, BusinessObjects)

- More than 246000 customers worldwide
- 86% of Forbes 500
- 85% of Fortune 2000 Oil and Gas

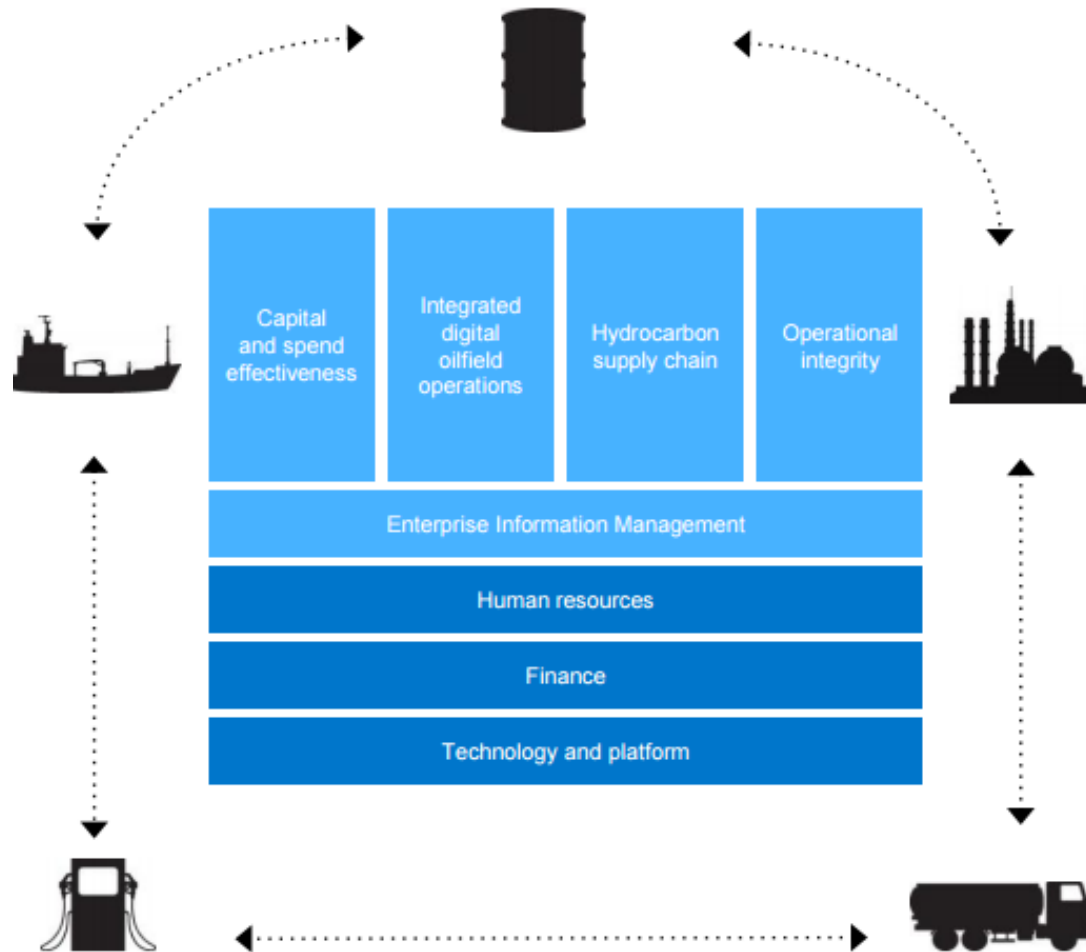
## Oracle (EBS, Peoplesoft, JDE, Siebel)

- 100% of Fortune 100

- **Espionage**
  - Theft of Financial Information
  - Trade Secret theft
  - Supplier and Customer lists theft
  - HR data theft
  - Other Corporate Data theft
- **Sabotage**
  - Denial of service
  - Modification of financial statements
  - **Access to technology network**
- **Fraud**
  - Modification of master data
  - Human Errors

According to SAP:

*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.*





Capital and Spend Effectiveness	Integrated Digital Oilfield Operations	Hydrocarbon Supply Chain	Operational Integrity
Capital Planning	Hydrocarbon Production Management	Hydrocarbon Supply and Distribution	Risk Analysis and Governance
Portfolio and Project Management	Hydrocarbon Revenue Management	Hydrocarbon Processing Visibility	Workforce Competency
Strategic Sourcing and Supplier Management	Field Logistics	Commercial Sales and Marketing	Asset Integrity
Procure To Pay and Business Network		Secondary Distribution and Fuels Retailing	Environment, Health, and Safety
		Convenience Retailing	

## Advantages:

- Improving supplier relations
- Reducing the cost of processing supplier invoices
- Enhancing visibility and transparency

## Risks:

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

## Applications:

- SAP PPM

## 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*



## Advantages:

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



- Tanks are maintained in the system as storage objects that reflect storage location stocks.
- One or more tanks can be defined at storage location level.
- A prerequisite for that is that the storage location is defined in Industry Solution Oil & Gas (Downstream) customizing as a tank storage location.
- You can make that setting by choosing HPM<sup>®</sup> Silo/Tank Management<sup>®</sup> Master Data<sup>®</sup>
- Define storage location as storage location for silo/tank management.
- The characteristics of the tanks are defined as storage object characteristics.
- The following data is stored in the tank master data
  - Capacity of a tank (maximum capacity)
  - Allowable impurity quantity
  - Allowed mass
  - Throughput quantities

## Advantages:

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

## Risks:

- Access control for 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)

- Asset Optimization – reduces production disruptions by enabling predictive maintenance
- Records maintenance history and identifies potential problems
- Condition monitoring is used for large rotating apparatus (turbines, compressors, pumps)
- Work order procedure is automatically initiated in the CCMS
- SAP Solution – SAP EAM

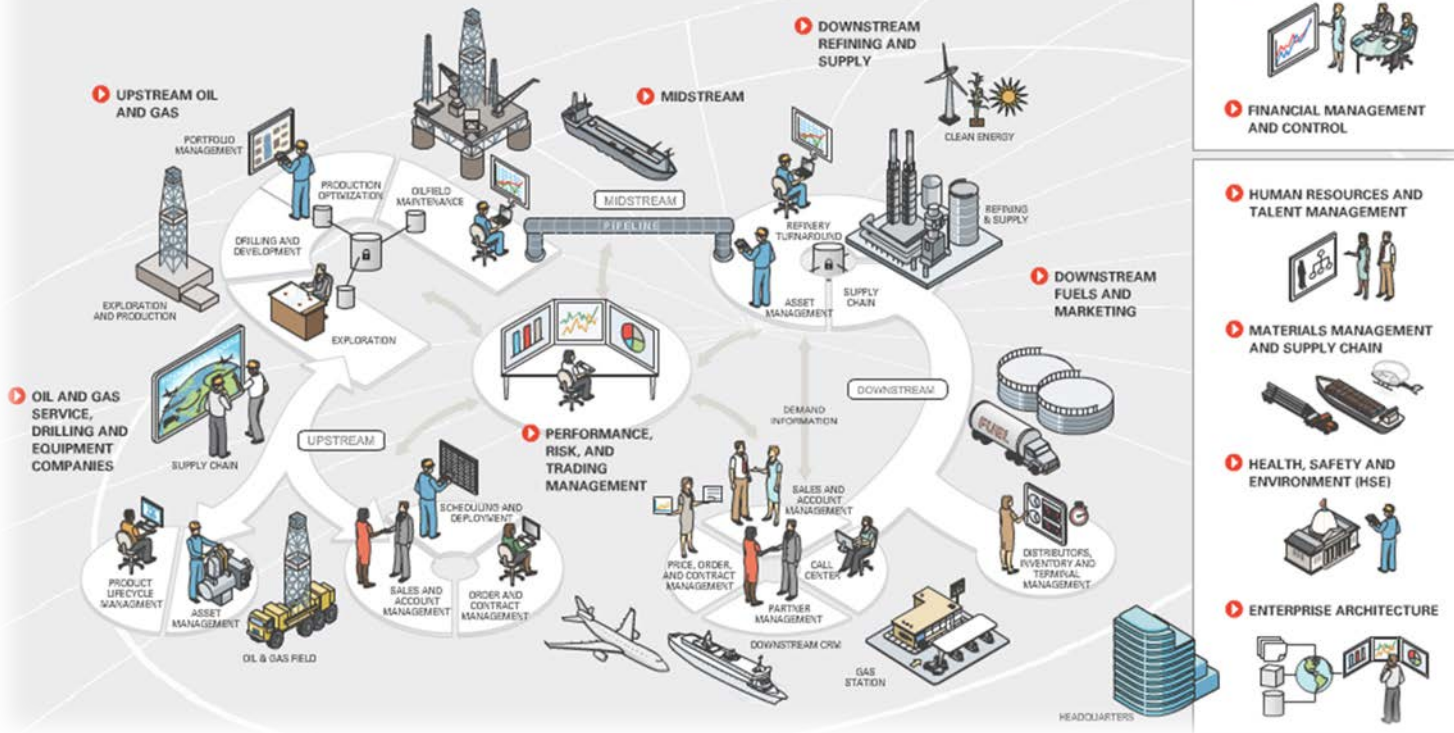


## Information-Age Applications for Oil and Gas

[Download PDF](#) | [E-mail This Page](#) | [Contact Oracle](#)

Oracle offers a complete, integrated set of solutions to meet the complex needs of the oil and gas industry. In addition, we provide access to information and tools to help anticipate changing market conditions—and the flexibility to respond to them effectively.

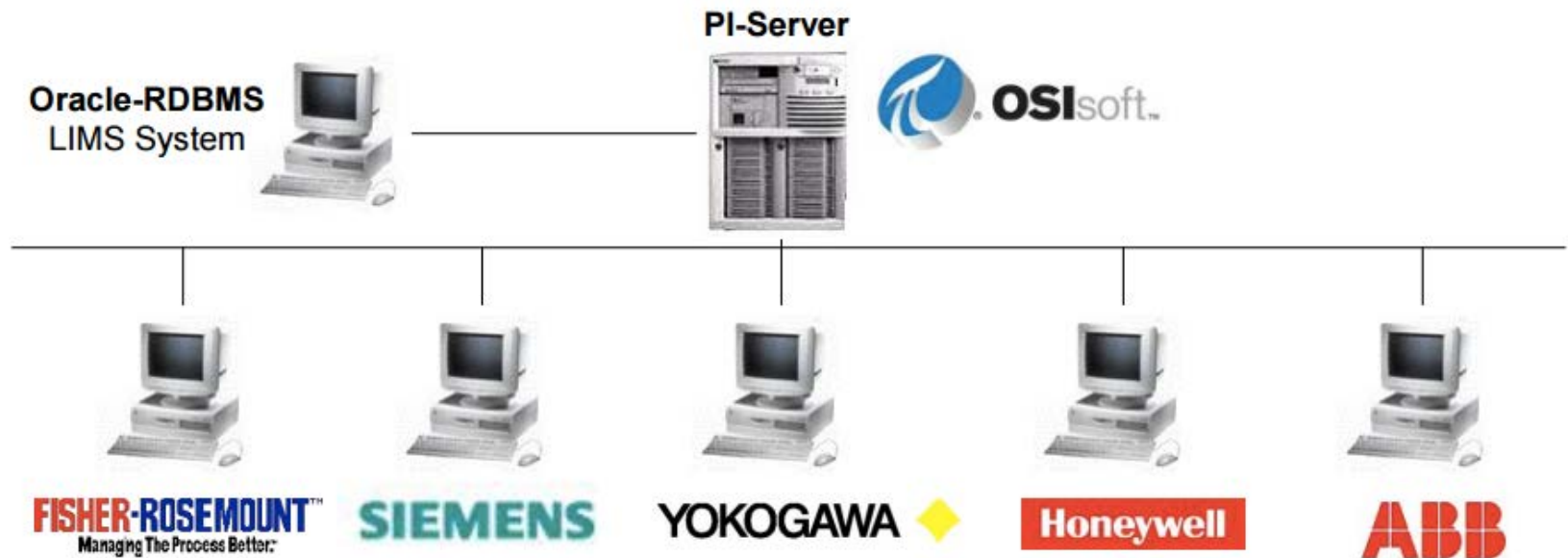
Click on each step of the lifecycle process below.



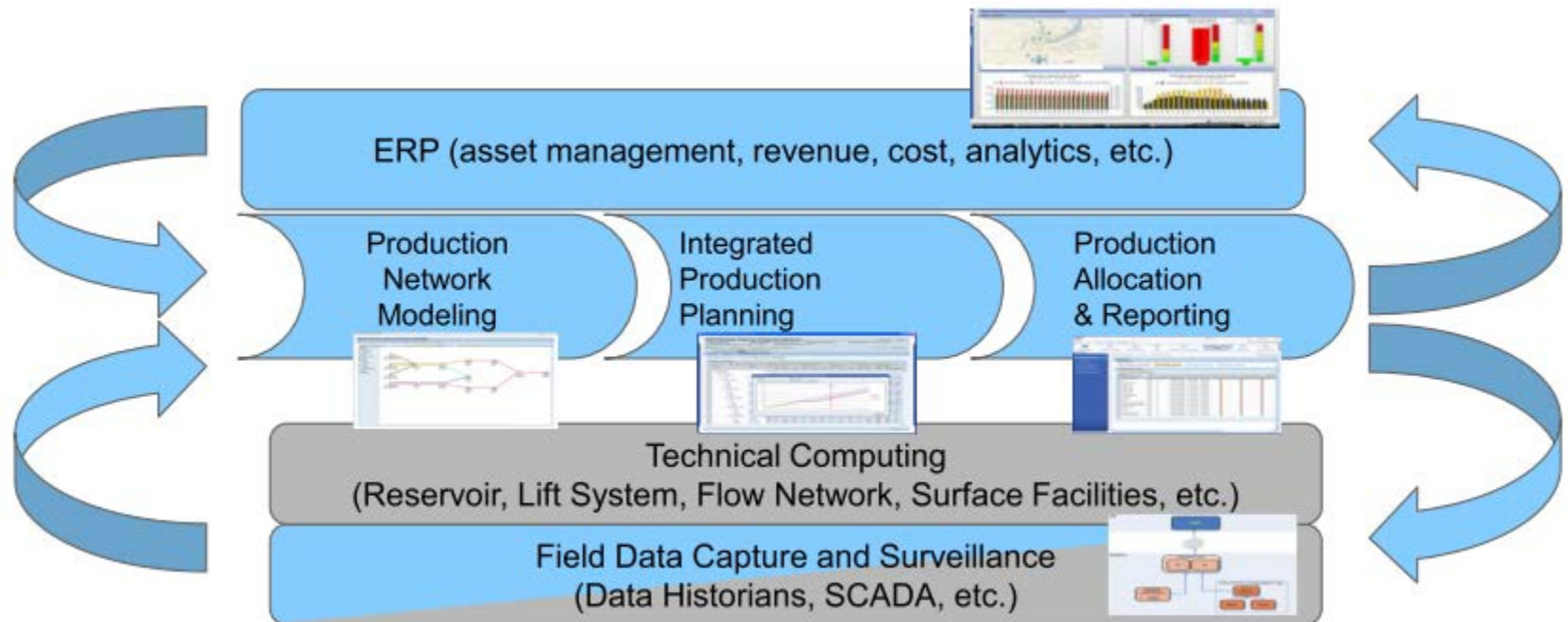
<http://www.oracle.com/ocom/groups/public/@ocom/documents/webcontent/oil-gas.html>

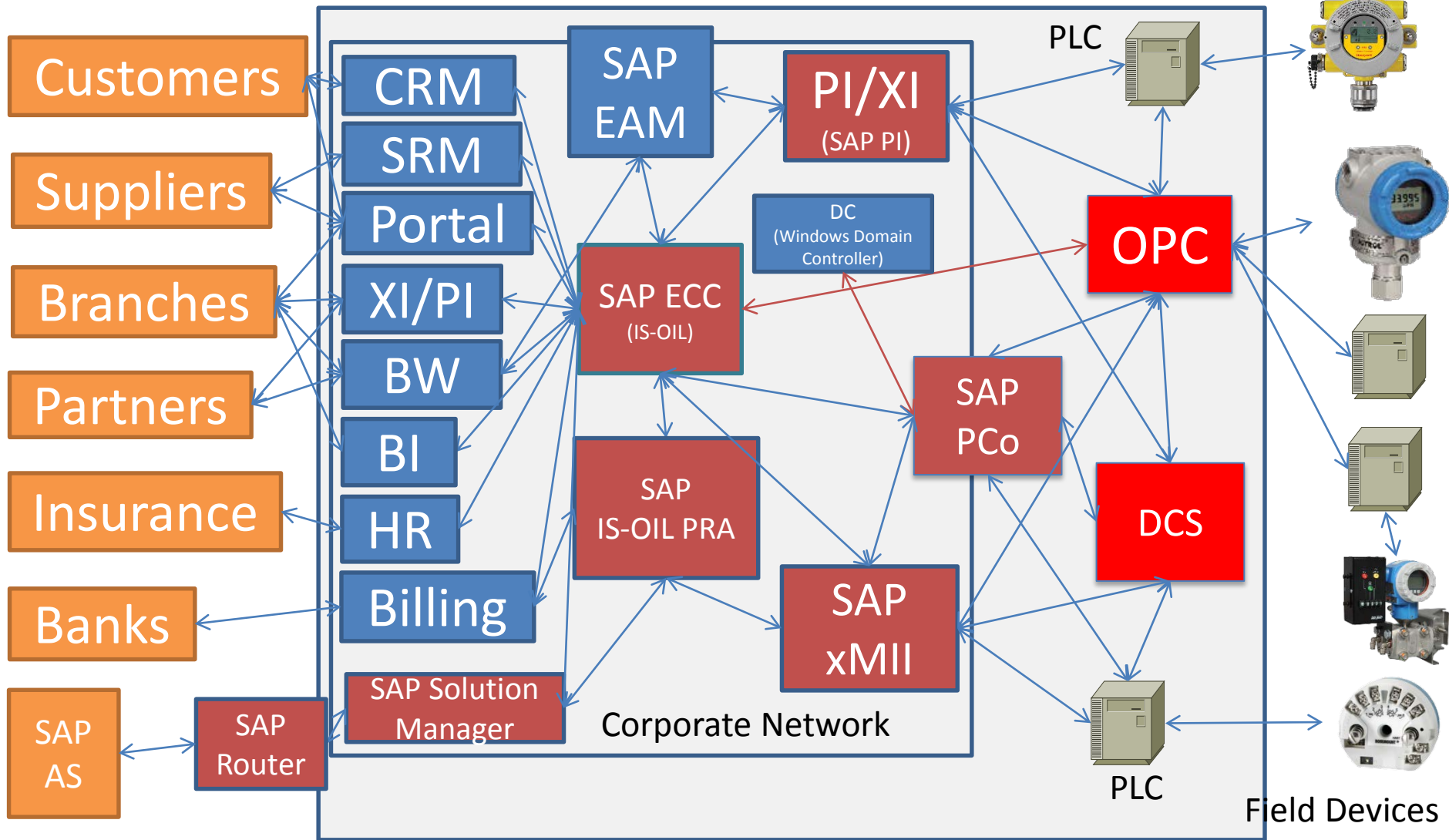


I think there is no need for details.



- Enterprise project portfolio management <- Exploration
  - SAP PPM, Oracle Primavera, MS Project, MS SharePoint
- Asset Lifecycle Management <- Refinery, Separation
  - SAP EAM (+AssetWise APM), Oracle EAM, Avantis, 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
- Advanced Metering Infrastructure (AMI) <- Fiscal Metering
  - SAP AMI





## Attacking Oil and Gas

## From the Internet to CORP

- 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-Business-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 in the Internet
  - <http://erpscan.com/wp-content/uploads/publications/SAP-Security-Attacking-SAP-clients.pdf>

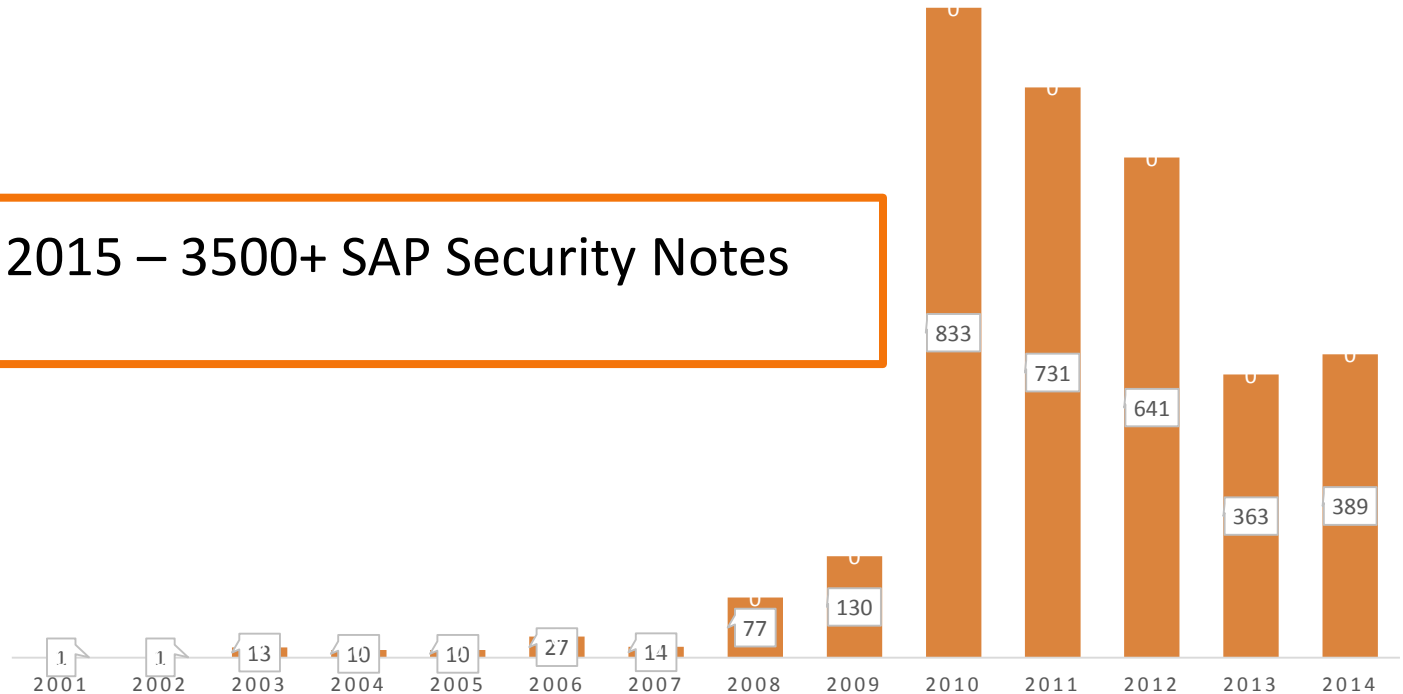
## From Corp to ERP



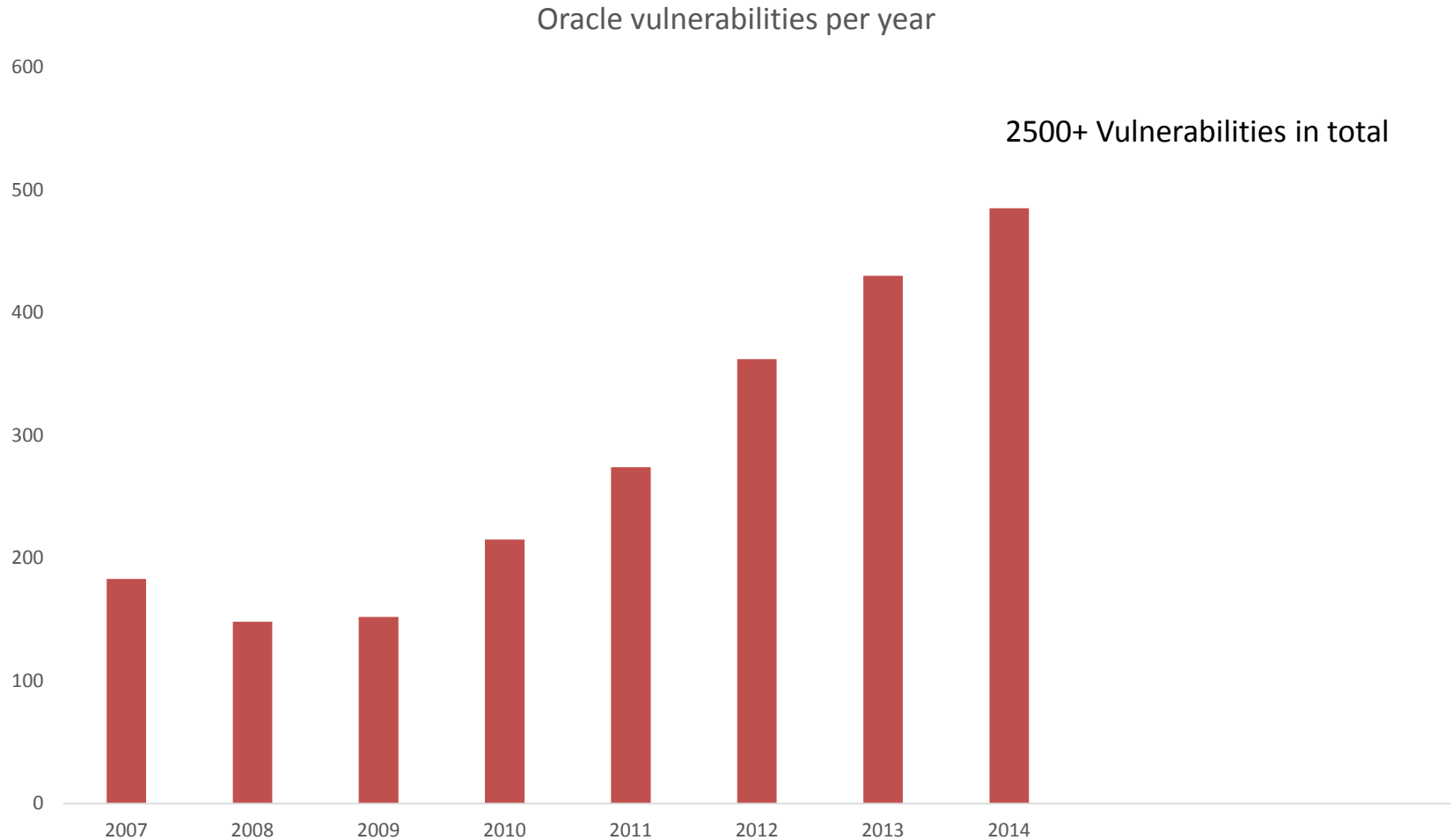
Numerous ways how an ERP system can be compromised:

- Vulnerabilities
- Misconfigurations
- Unnecessary privileges
- Custom code issues

By October 2015 – 3500+ SAP Security Notes



Only one vulnerability would suffice  
to jeopardize ALL business-critical data



- ~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.**

**<http://erpscan.com/wp-content/uploads/publications/EASSEC-PVAG-ABAP.pdf>**

Domain specific languages in business applications (ABAP, PeopleCode, XSJS, X++) can have vulnerabilities as well as backdoors left by 3<sup>rd</sup> party organizations:

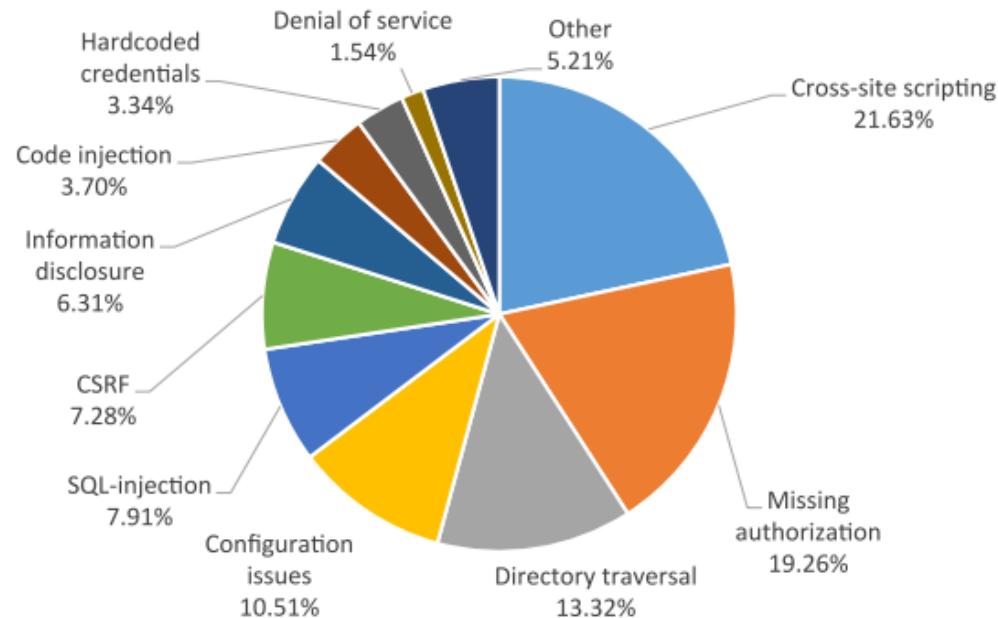


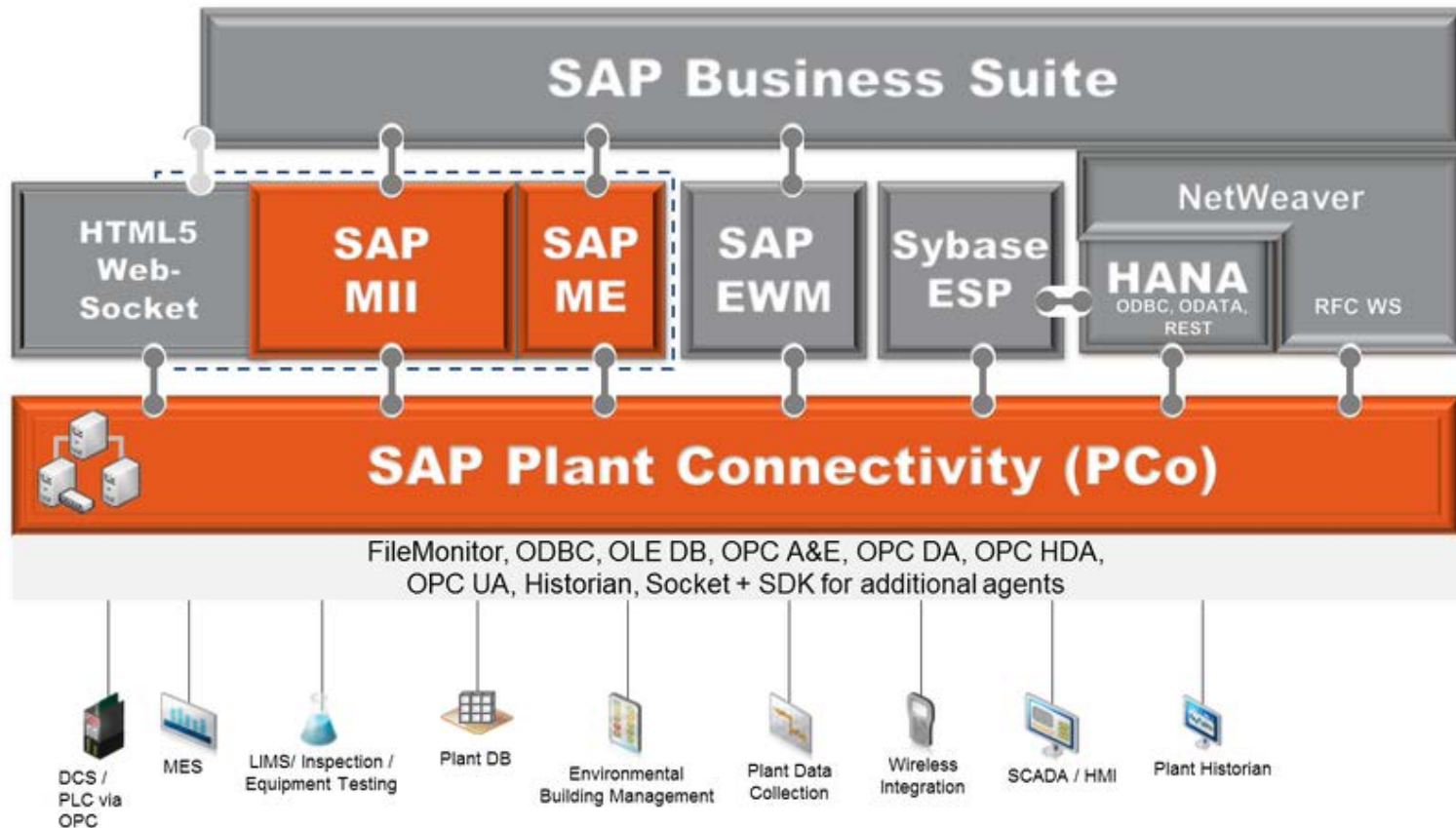
Figure 3.4-1 TOP-10 SAP Security Vulnerabilities, sorted by type

<http://erpscan.com/wp-content/uploads/publications/3000-SAP-notes-Analysis-by-ERPScan.pdf>

### Critical privileges and SoD issues

- For example: Create vendor + Approve payment order
- Usually  $((\sim 100 \text{ Roles} \times 10 \text{ actions})^2)/2 = 500k$
- 500k potential conflicts for each user!
- A lot of work to do
- Usually, it takes two years to decrease the number of conflicts from millions to hundreds.
- And you still will be vulnerable

## From ERP to OT





- **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 configuration

Finally, we need to find a way to hack

- **SAP HANA**
- **SAP xMII**
- **SAP PCo**

- SAP HANA can store the most critical data form Plant for analytics
- It is a database used by many SAP and non-SAP applications
- Some of them store critical data for analytics

SAP HANA can store the most critical data form Plant for analytics

- Connections with other systems (ERP, LIMS, Custom)
- **SAP RFC connections**
- **SAP HANA Vulnerabilities**

- **[ERPSCAN-15-024] SAP HANA hdbindexserver – Memory corruption**
- An anonymous attacker can use a special HTTP request to corrupt SAP HANA index server memory.
- An attacker can use vulnerability to execute commands remotely without authorization, under the privileges of the service that executes them.
- CVSS: 9.3
- <http://erpscan.com/advisories/erpscan-15-024-sap-hana-hdbindexserver-memory-corruption/>
- <http://www.fiercitsecurity.com/story/security-holes-rise-sap-hana-big-data-platform-warns-erpscan/2015-10-15>

Some systems should be connected at least on the network layer

- SAP RFC links from ERP to xMII
- NetWeaver J2EE Platform vulnerabilities (core of xMII)
- **Direct SAP XMII vulnerabilities**
- Database links to xMII
- Shared SSH keys
- Similar passwords
- Others

- MII: Manufacturing Integration and Intelligence
- Connects manufacturing with enterprise business processes, providing information to improve production performance
- On top of SAP Netweaver J2EE (with its vulnerabilities)
- xAPPs technology exposes web services and data from multiple systems
- **Located on the corporate network**
- `xapps~mi~ears` is the main application with several endpoints accessible at <http://server:50000/XMII>
- Has some vulnerabilities (Blind SQLi/XXE) [can't disclose details]

- We have Admin access, but how to execute OS commands?
- In «Log viewer» we chose «Connect to Remote System»

**Log Viewer: Overview**

Favorites ▾ Related Links ▾ Go To ▾ [Support Details](#)

View ▾ Log Files ▾

Open View ...

Open Expert View

**Connect to Remote System**

Set As Default View

Save View

Save View As ...

Delete View

Export View ...

Import View ...

Customize Layout

About Current View

Expand All Related Logs ▾

	Time	Message
nm-dd		
09-28	11:46:25:...	Session Information [1 active users, 1 unique users]
09-28	11:41:59:...	LOGIN.OK User: Administrator IP Address: 172.16.30.9 Authentication Stack: sap.com/xapps~xmii~ear*XMI Authentication Stack Properties:...
09-28	11:26:59:...	LOGIN.OK User: Administrator IP Address: 172.16.30.9 Authentication Stack: sap.com/xapps~xmii~ear*XMI Authentication Stack Properties:...
09-28	11:16:25:...	Session Information [2 active users, 1 unique users]
2015-09-28	11:11:59:...	LOGIN.OK User: Administrator IP Address: 172.16.30.9 Authentication Stack: sap.com/xapps~xmii~ear*XMI Authentication Stack Properties:...



**Log Viewer: Overview** Restore Default View | Back Forward | History | Home | Help | Log Off

Favorites | Related Links | Go To | Support Details Search: log viewer Go

View | Log Files

**Connect to Remote System**

**Remote Connection**

<input type="checkbox"/>	<input type="text" value="Connect to host"/>	<input type="text" value="172.16.2.24"/>	<input type="text" value="On Port: 50013"/>	<input type="text" value="Protocol: SAP Instance Agent"/>	<input checked="" type="checkbox"/>	<input type="button" value=""/>
<input type="checkbox"/>	<input type="text" value="Define New Connection"/>					

We enter the IP of a machine controlled by us  
It will connect back to my laptop with something...

[illegible]

## Request contains Basic Authentication header

We decode it as user « {221....} » and password  $x^{*****}x$

The password is random and lives max. the JVM lifetime

- Welcome to built-in SAPControl accounts, this one is used in the context of *TrustedInternalConnections*
- Usually, the SOAP endpoint on tcp 50013/1128 is used with OS credentials, but there are exceptions ;-)
- SAPControl SOAP function `OSExecute()` remotely is granted with that special user
- miiadm OS execution rights, abuse ?
- dump sensitive files like `SecStore.*` → get Sybase sa account
- Dump backdoor, get remote shell
- Real pentest of PCO begins

SAP Plant connect usually stays between SAP xMII and Critical device

- Connections with other systems (MES, LIMS, Custom)
- **SAP xMII connections (password decryption)**
- SAP PCo vulnerabilities
- **Domain credentials (If improperly secured)**
- Database links
- Shared SSH keys
- Similar passwords

- SAP Plant Connectivity
- Bridge between the industrial world and SAP Manufacturing modules
- Windows box, .NET application
- Usual pipeline Source → Processing → Destination
- Source: OPC server (MatrikonOPC, Siemens Simatic, KEPServerEX) or DCS (???)
- Destination: SAP HANA, SAP XI, SAP xMII, LIMS, DB...
- Agent: Windows service that does the polling



**Steve Stubbs** Aug 18, 2014 5:48 PM (in response to darshan sheth)

**Helpful Answer** Re: Switching Kepware servers in PCO

Darshan,

For DCOM to work with PCo and Kepware, you have 2 options to configure the user access:

1. Allow full DCOM access for domain users that are members of the server Administrators group, EVERYONE, SYSTEM and NETWORK, and allow PCo and Kepware services to run under LocalSystem account (some network admins will not allow this as it opens potential network security holes)
2. Define named users or named Domain Group permissions for DCOM.
  - 2.1. Use the named user or users that are members of the named Domain Group for the following:
    - named user for Kepware server\_runtime service
    - named user for PCo Agent Instances
    - administrative user to log into PCo remote Desktop

Avoid hosting PCo and remote OPC Servers on different Domains or on Workgroups -- should always be in the same Domain.

I strongly recommend that you migrate to Kepware V5 and investigate using the Kepware OPC UA interface along with PCo OPC UA Agent where you are going to have remote OPC Server requirements, and avoid the DCOM issues altogether.

Installing Kepware on PCo server, or PCo on the Kepware server will remove any DCOM configuration requirements.

Regards, Steve



**Eswaraiah Manda**

Mar 21, 2013 8:27 PM

## OPC server connectivity issue from SAP MII 12.1

This question is **Assumed Answered**.

Hello Experts,

I have a Requirement to connect an OPC server from sap MII 12.1 to get the data in form of tags

We are using RSView 32 OPC server ,

I came across through some posts that PCo has the ability to connect

I tried using PCo connection connecting the source system , but I am unaware whether my source system is connected successfully or not  
My destination to MII system is successful

Can we get all the tags to which source system(RS View 32 sacada system) PCo is connected in PCo management console.

- We have Admin access to xMII
- Table SAPSR3DB.XMII\_SERVERPROP contains the user/pass of PCo when in the «Query Process» mode
- Password is 3DES encrypted. Where is the key?
- SECURE\_STORE\_KEY is a handle for our application to the Java SecureStorage
- Inside the SecureStorage is our crypto Key

- Idea: Decrypt the password with a JAVA PoC using the existing logic (jars)
- Problem :
- SecureStorage is inside server JVM instance
- Not exposed to the outside
- Connect through ICMAN service (gateway to the Netweaver JVMs)
- Protocol P4 remotely accessible on TCP/50004
- Finally, we can get a context and `ctx.list()` the services, see SecureStorage
- When `ctx.lookup()`, the handle on the SecureStorage is always NULL: why?



From SAP support forum

- *«Secure storage is protected by call stack validations. It can only be called from permitted connections, such as Jco.»*

No JCo connections on the system.

Seems like a dead end :-(

Wait...

**Welcome Administrator1, 11111**

**SAP MII: Encryption Configuration**

Edit Save Cancel

Choose Encryption Algorithm: TripleDES

System Management

Security Services

[Data Access](#)

[Encryption Configuration](#)

[Credential Stores](#)

[User Management](#)

Data Services

Content Development

Catalog Services

Message Services

Alerts and KPI

System Resources

Support

ERP-Shop Floor Integration

Worker UI Management



**Welcome Administrator1, 11111**

System Management

Security Services

- Data Access
- Encryption Configuration**
- Credential Stores
- User Management

Data Services

Content Development

Catalog Services

Message Services

Alerts and KPI

System Resources

Support

ERP-Shop Floor Integration

Worker UI Management

**SAP MII: Encryption Configuration**

☒ Encryption configuration was saved successfully

Edit Save Cancel

Choose Encryption Algorithm: Base64

- TCP/50050 : SOAP remote administration interface is offered by `pcohostsvc.exe` (Windows service manually started)
  - Start/Stop instance, dump configuration
- TCP/9000 : by default without authentication
  - «Active Queries» to the PCo instance via xMII protocol (XML)
- TCP/445: For Domain Access
  - Full access to PCo. Just use our login/pass from xMII

- Traffic modification: attacks based on the fact that the MII-PCo connection is not authenticated by default:
    - Fake PCo
      - Kill the actual PCo and show that everything is OK in MII
      - MITM + selective modification
      - Steal your oil, but tank level doesn't change
    - Protocol attack
      - MII = requests over XML
      - Protocol parsing on the PCo side
- CDATA forwarded to the sources (OPC UA/DA)
- Exploitation of the source via this channel?

**Now we are inside your OT network and can do whatever we want, there is no Air Gap!**

SAP Plant connect interacts with DCS/OPC

- **On the same workstation**
  - Required when configuring some DCS/SCADA systems
- **On the same network**
  - OPC vulnerabilities
    - KEPServerEX Resource exhaustion <https://ics-cert.us-cert.gov/advisories/ICSA-15-055-02>
    - KEPServerEX Input Validation <https://ics-cert.us-cert.gov/advisories/ICSA-13-226-01>
    - MatrikonOPC Gateway DoS <https://ics-cert.us-cert.gov/advisories/ICSA-13-106-01>
    - MatricanOPC DoS (0-day)

DCS/SCADA can control PLC

- **Attack PLC using access to DCS/SCADA**
- **Attack PLC via PLC vulnerabilities**
  - ABB AC500
    - ICSA-12-320-01 : ABB AC500 PLC Webserver CoDeSys Vulnerability





## DEMO

**How does one go about securing it?**

- Protect your ERPs and other business applications
- Review all connections
- Secure connections where possible
- And please, don't include critical systems to domain

## **Business security (SoD)**

*Prevents attacks or mistakes made by insiders*

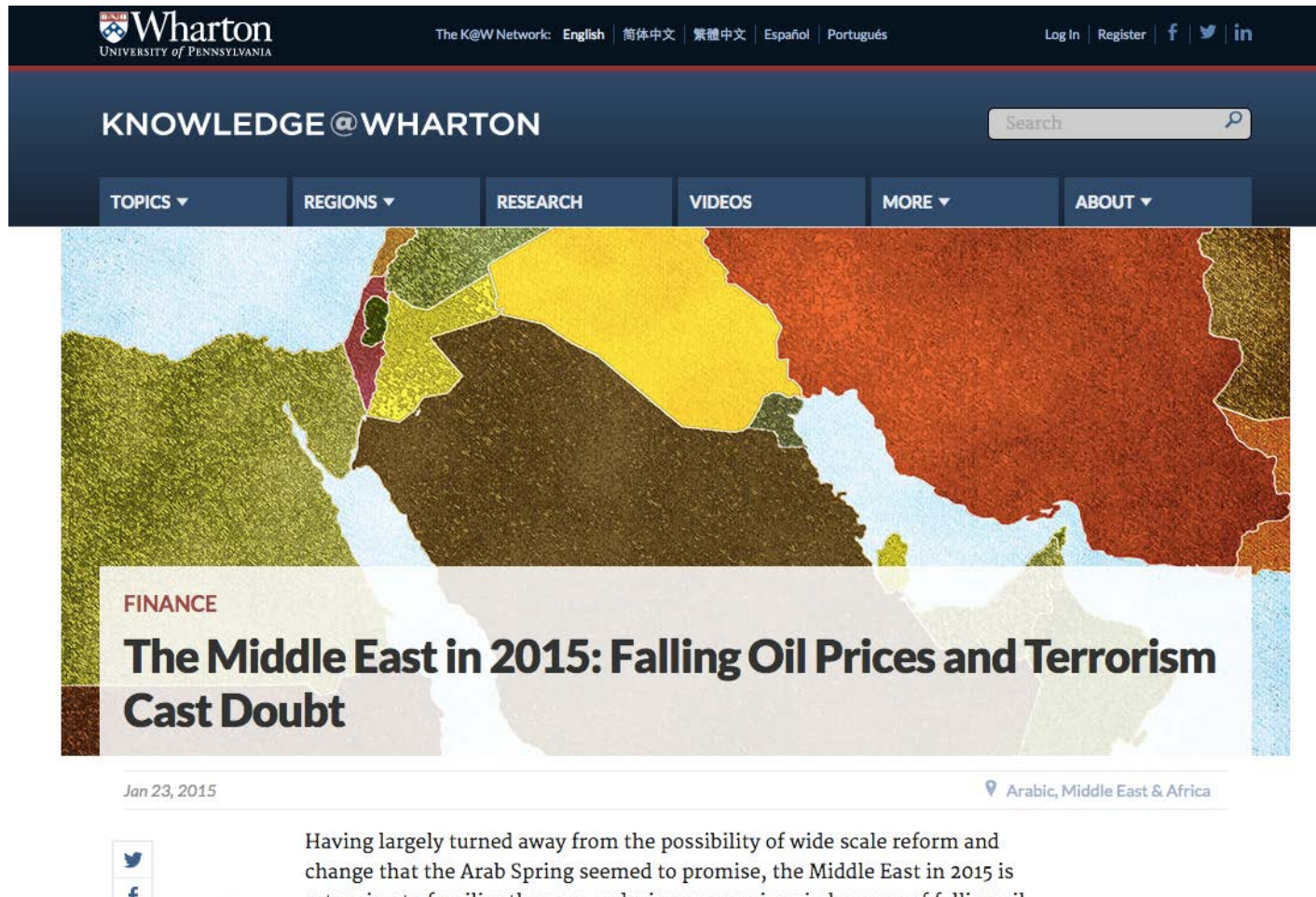
## **Code security**

*Prevents attacks or mistakes made by developers*

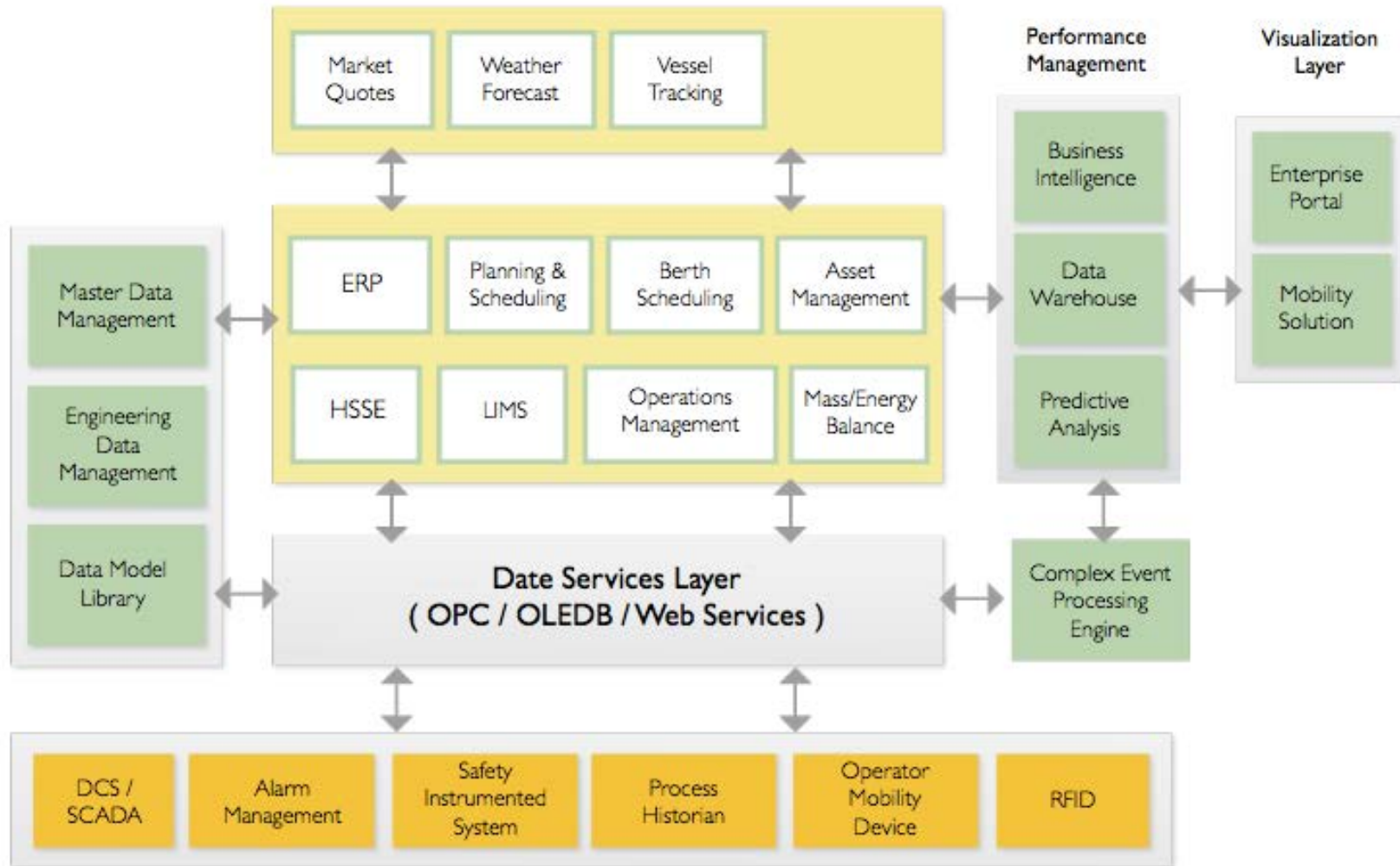
## **Application platform security**

*Prevents unauthorized access both within corporate network and from remote attackers*

Every attack on a system have a significant impact



The screenshot shows the Wharton Knowledge@Wharton website. The header includes the Wharton University of Pennsylvania logo, language options (English, 简体中文, 繁體中文, Español, Português), and links for Log In, Register, Facebook, Twitter, and LinkedIn. Below the header is a search bar and a navigation menu with categories: TOPICS, REGIONS, RESEARCH, VIDEOS, MORE, and ABOUT. The main content area features a map of the Middle East with a color-coded overlay. A text box over the map contains the article title "The Middle East in 2015: Falling Oil Prices and Terrorism Cast Doubt" under the "FINANCE" category. Below the title, the date "Jan 23, 2015" and the location "Arabic, Middle East & Africa" are displayed. A snippet of the article text is visible: "Having largely turned away from the possibility of wide scale reform and change that the Arab Spring seemed to promise, the Middle East in 2015 is returning to familiar themes: enduring economic pain because of falling oil".



- Researchers - now you know where to start from, Oil and Gas security is a small universe.
- Pentesters - now you know how to break into the most critical network and impress decision makers.
- CISOs - now you know that there is no Air Gap between IT and OT and what you need to check.

[a.polyakov@erpscan.com](mailto:a.polyakov@erpscan.com)

@sh2kerr

[m.geli@erpscan.com](mailto:m.geli@erpscan.com)

228 Hamilton Avenue, Fl. 3,  
Palo Alto, CA. 94301

USA HQ

Luna ArenA 238 Herikerbergweg,  
1101 CM Amsterdam

EU HQ

[www.erpscan.com](http://www.erpscan.com)  
[info@erpscan.com](mailto:info@erpscan.com)