Invest in security to secure investments

ERPScan
Security Solutions for SAP

SAP Cyber Security for Oil and Gas

Alexander Polyakov - CTO, ERPScan
Mathieu Geli - Head of SAP Threat Intelligence, ERPScan

About 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

- 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

Attention!!!

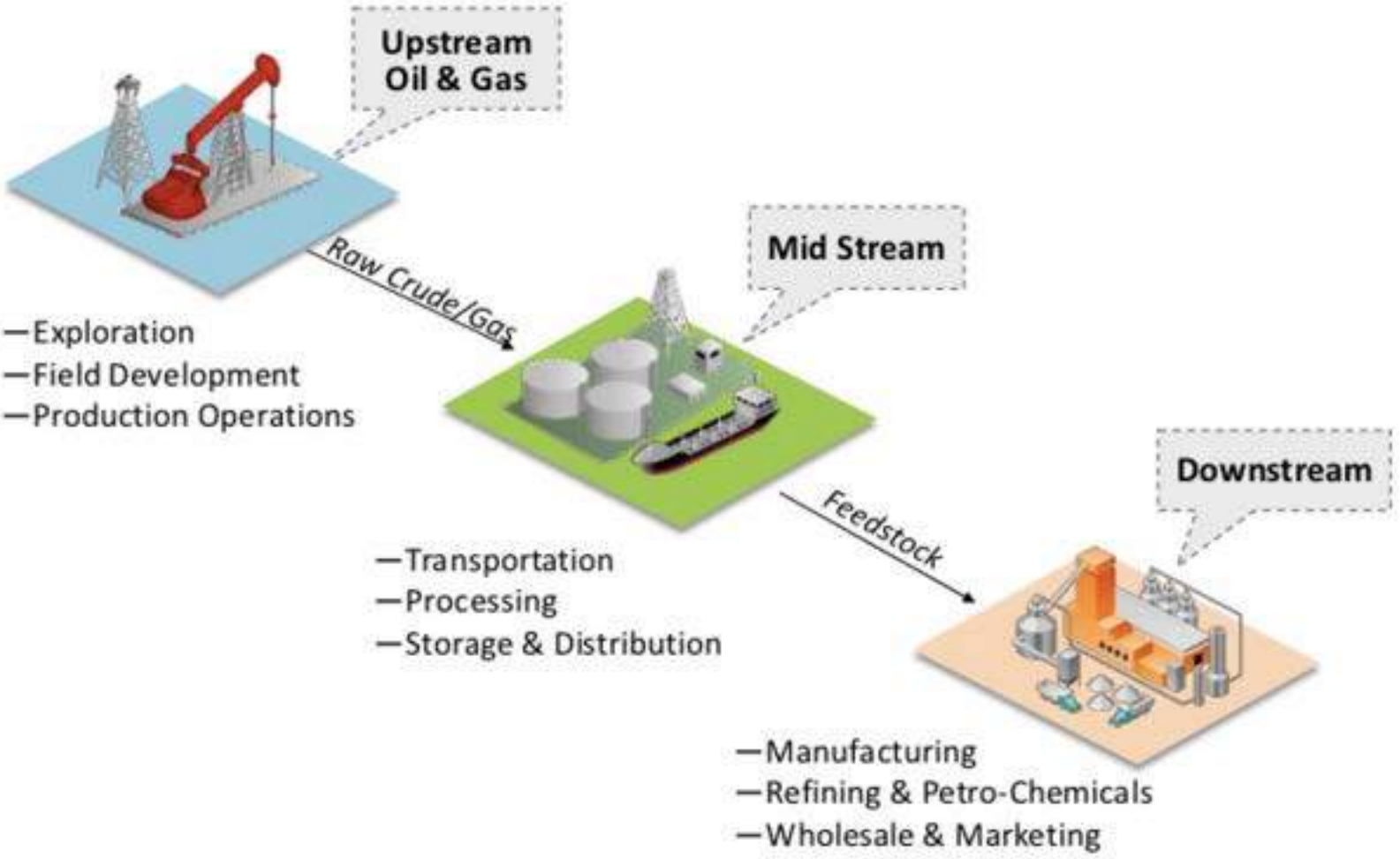
- This is NOT a traditional type of talk
- For me neither
- There are more questions than answers
- There is the first technical Oil and Gas Cyber Security talk
- This is just a beginning

Oil and Gas 101

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.

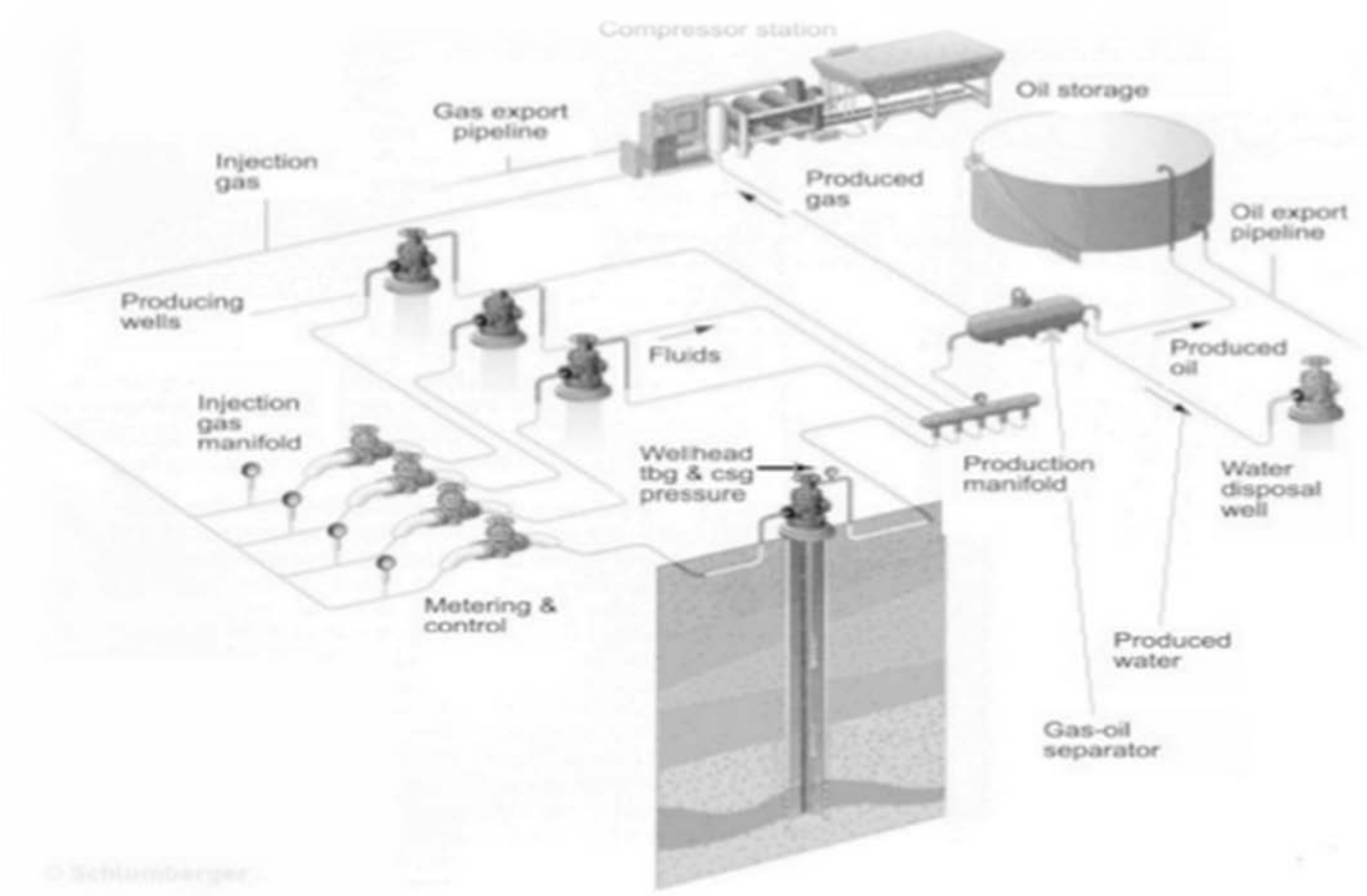
Oil and Gas 101



Upstream: Critical processes and systems

- Extraction (Drilling)
  - Drilling Control Systems, Pump control Systems, blow-out prevention systems, Flare and Vent disposal control systems
- Gathering (From earth to separators)
  - Well Monitoring Systems, Manifolds management systems, Net oil measurement systems
- **Separation (Separate oil, gas and water)**
  - Gas Oil Separation Plant, Heaters, Combustion Control Systems, **Burner Management systems**, Compressor Control Systems, Emergency Shutdown Systems, Vibration Monitoring Systems, Distribution Control Systems for Coalescence and Desalting
- Gas compression (Prepare for storage and transport)
- Temporary Oil Storage (Temporarily store before loading)
- Waste disposal (Water disposal)
- **Metering (Calculate quantity before loading)**
  - **Fiscal Metering Systems**, Liquid Flow Metering systems, Gas Flow Metering Systems, Wet Gas Metering Systems

Typical Upstream processes (Onshore)

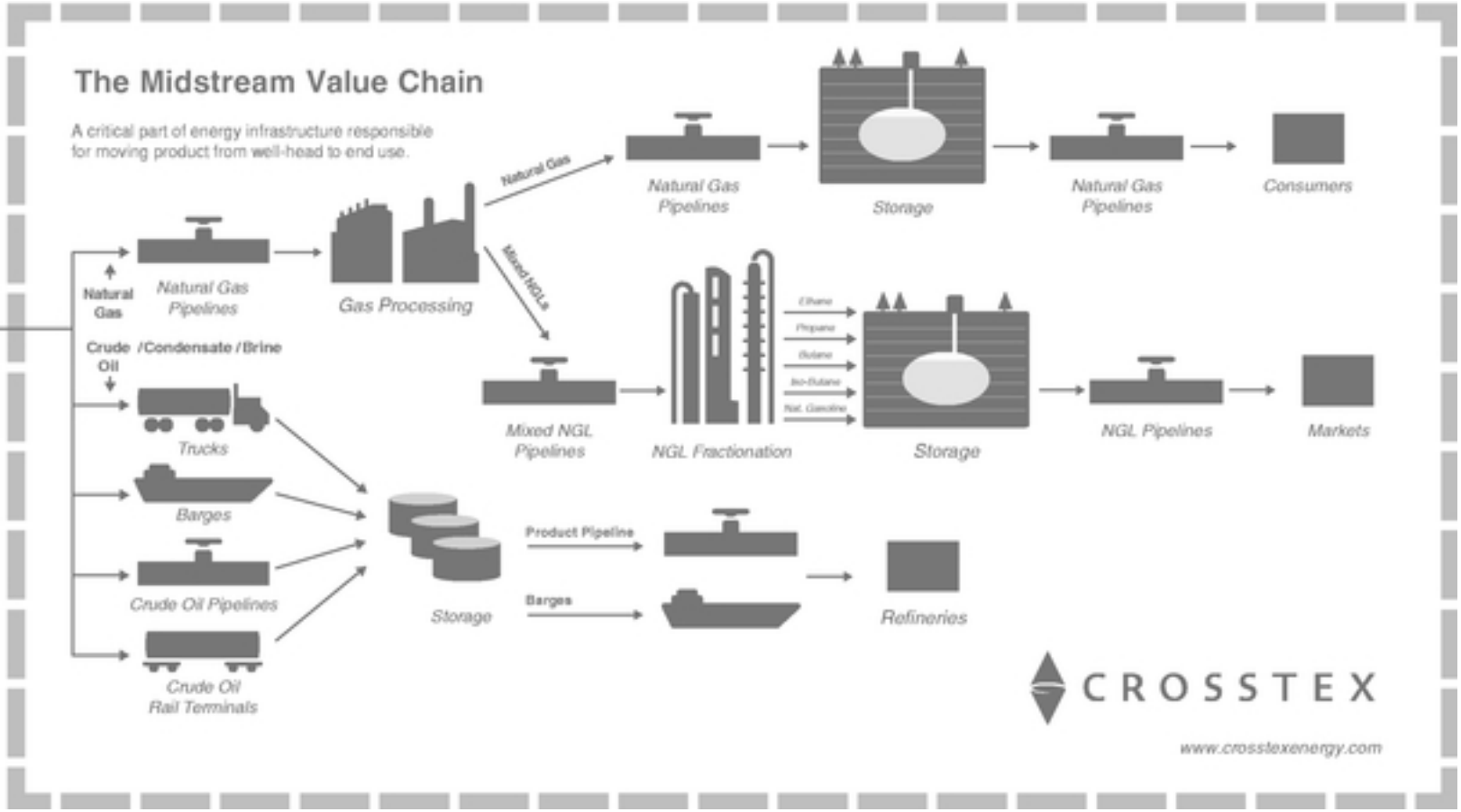


Simple Upstream oil and gas process

Midstream: Critical processes and systems

- Terminal management (Obtain oil from upstream)
  - Metering, Movement Automation Systems, Order Movement Management Systems
- Gas Processing (Separate natural gas and NGL)
- Gas Transportation (Transfer gas to storage)
  - Pipeline management SCADA
- Oil transportation (Transfer oil to storage)
  - Pipeline management SCADA
- Base load Gas storage (Temporary and long-term)
- Peak load Gas Storage
- LNG Storage
- **Oil Storage (Long-term oil storage)**
  - **Tank inventory systems,** Tank Temperature management, Tank Gauging Systems, Product Movement

Midstream 101



Downstream: Critical processes and systems

- Refining (Processing of Crude Oil)
  - Refinery Management Systems, Blend Control/Optimization systems, Movement Automation Systems, Emission Monitoring Systems
- Oil Petrochemicals (Fabrication of base chemicals and plastics)
- Gas Distribution (Deliver gas to utilities)
- Oil Wholesale (Deliver petrol to 3rd parties)
- Oil Retail (Deliver petrol to end users)
  - Truck loading Automation, Gas Pump Monitoring Systems, POS

What can happen?

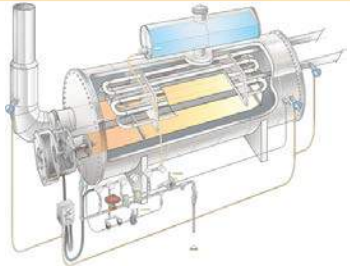
Plant Sabotage/Shutdown
Equipment damage
Utilities Interruption
Production Disruption (Stop or pause production)
Product Quality (bad oil and gas quality)
Undetected Spills
Illegal pipeline taping
Compliance violation (Pollution)
Safety violation (Death or injury)

Some critical processes in Oil and Gas: details

SEPARATION (GOSP)

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

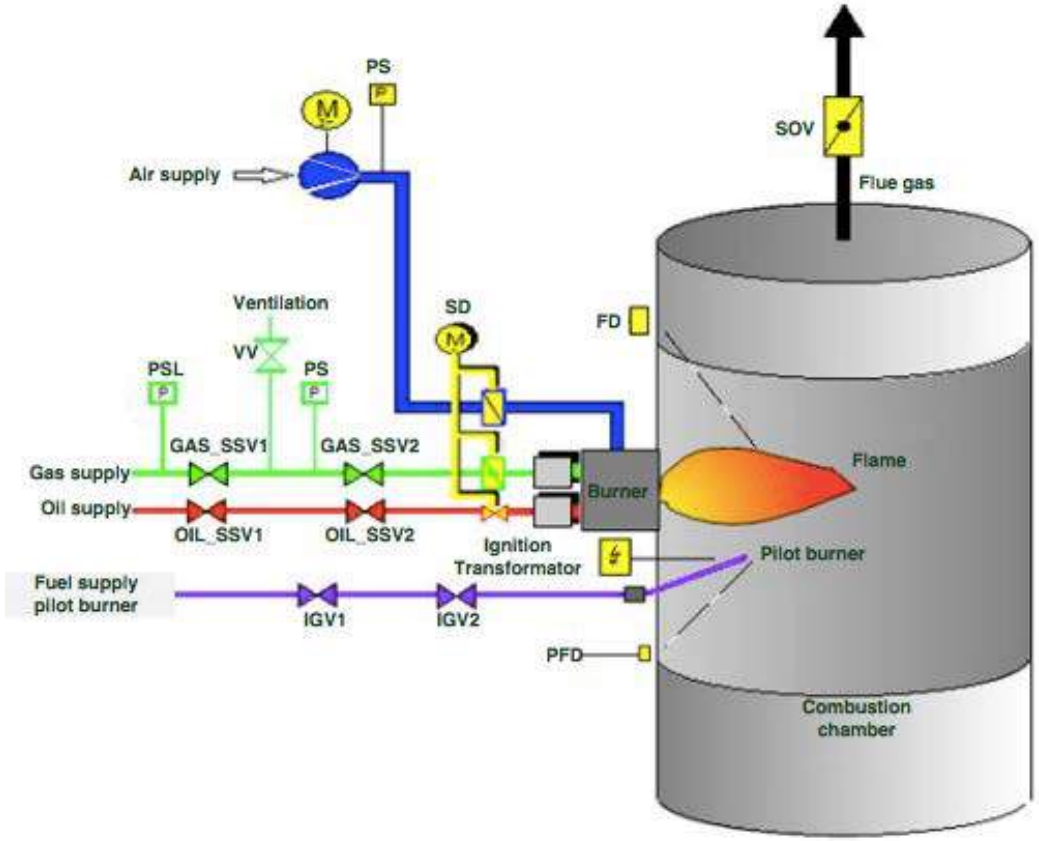
SEPARATION: Burner Management System (BMS)



- Burner Management System
- Used in a variety of applications:
  - **Separators**, tanks, heaters, Incinerators, flare stacks, etc.
- Management systems: (easy to manipulate)
  - **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

Simple Burner Management System

Designitions	Definition
IGV1	Pilot gas valve 1
IGV2	Pilot gas valve 2
OIL_SSV1	Oil safety shut-off valve 1
OIL_SSV2	Oil safety shut-off valve 2
GAS_SSV1	Gas safety shut-off valve 1
GAS_SSV2	Gas safety shut-off valve 2
PSL	Gas pressure sensor lower limit
VV	Vent valve
FD	Flame detector
SD	Servo drive
PS	Pressure sensor
SOV	Shut-off valve
PFD	Pilot flame detector



https://cache.industry.siemens.com/dl/files/036/109477036/att_856487/v2/109477036_Burner_Application_Example_TIAP_DOC_v102_en.pdf

SEPARATION: Burner Management System (BMS)

OK, what if we have access to BMS?

What can we do?

Some physical attacks?

SEPARATION: Burner Management System (BMS)

- There are **three components in the fire triangle**. If one of these components is missing, the reaction cannot be sustained.
- Control of the **air/fuel ration is one of the most important** functions of combustion/burner systems. It must ensure that sufficient excess air is maintained.
- If fuel is missing, then the system is safe, but **if air or heat for ignition is missing, the situation is potentially dangerous.**
- To minimize the explosion risk, we have to ensure that flammable mixtures do not accumulate anywhere within the plant
- **If an attacker wants to commit sabotage and stop operations by destructing burning process, he needs to control any of the sources of flammable mixtures**

SEPARATION: Burner Management System (BMS)

Flammable mixture sources:

- Oil or gas leaking into the combustion chamber through the burner as a result of **leaking fuel shut off valves**.
- Deposits of coal or oil **not properly purged from the system.**
- Operation of the plant with **insufficient combustion air** resulting in CO and unburnt fuel in the downstream ducting and dust collector.
- Quenching of the flame **by cold dust entering the furnace**. Cold dust can reduce the temperature below the ignition temperature.
- Fuel entering the furnace as a result of **repeated unsuccessful ignition attempts**. This is the significant risk with oil firing, A typical cause is a cold oil remaining in pipes during a shutdown.

SEPARATION: Burner Management System (BMS)

- The burner management system performs a vital safety function, it prevents operator errors leading to danger and causes the safe shutdown of the burner in case of other equipment malfunction.
- The main function of the BMS is to allow and ensure the safe start-up, operation, and shutdown of the Fired Heater.
- Since BMS system manages all critical processes for burner safety, unauthorised access to BMS can lead to multiple risks including Explosion.
- The simplest attack on BMS System is to **turn off the purge**.
- As mentioned before, cold oil left in pipes during previous shutdowns can burn and damage the equipment.

METERING

- Risks:
  - Product Quality, Monetary loss
- Analyzes density, viscosity of 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

METERING: Fiscal Metering (Custody transfer)

- 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.
- A small error in measurement leading to financial exposure
- Typical pipeline is designed to pump 60,000 gallons of oil per minute.
- Over a year, the 0.1% error would amount to a difference of $50m.
- 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 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.

Fiscal Metering (examples)

- 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.

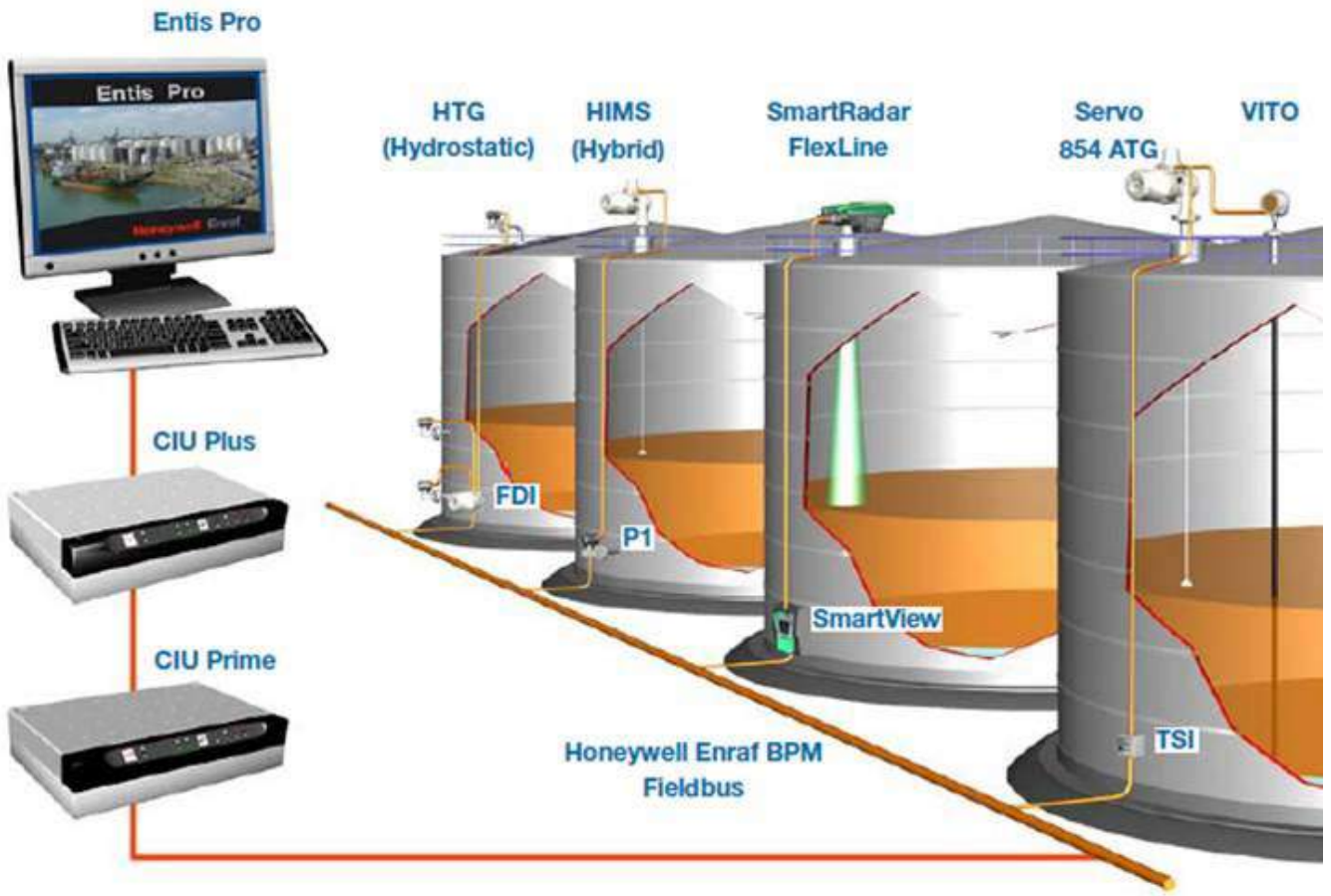
OIL STORAGE

- Risks
  - Plant Sabotage/Shutdown, Equipment damage, Production Disruption, Compliance violation, Safety violation
- Storage facilities usually consist of 10-100+ tanks with 1-50m barrels
- Managed by Tank Inventory Systems (TIA)
- TIS collects data from special **tank gauging systems** that are used to measure the level in storage tanks
- Accurate records of volumes and history are kept
- **Forecasting for stock control**
- Tank level deviations can result in hazardous events such as a tank overfilling, liquefied gas flashing, etc.

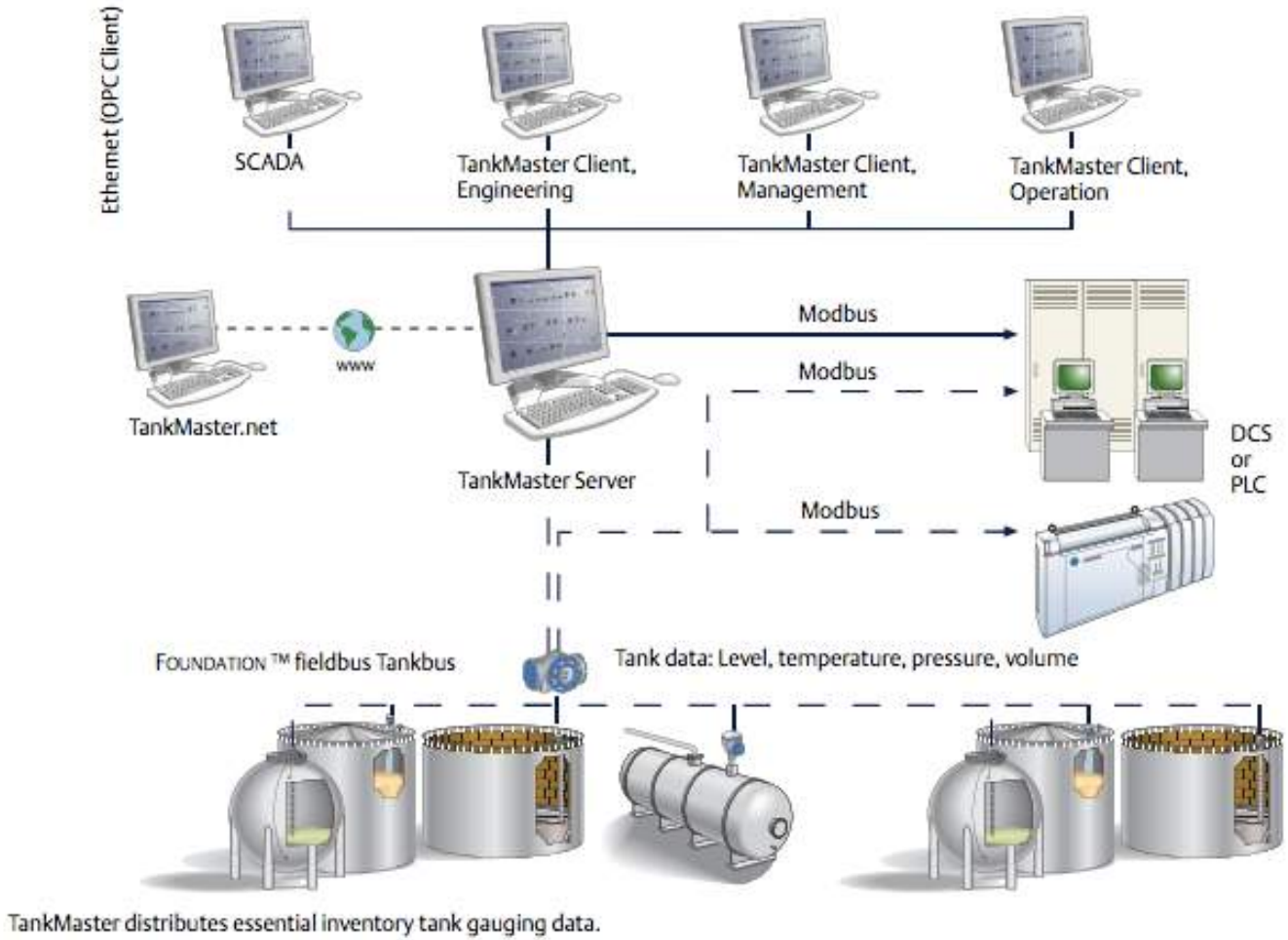
OIL STORAGE: Tank Inventory Systems (Details)

- Terminal Management
  - Honeywell Enfaf TM BOX **(connected with SAP)**
  - Emerson Syncade Terminal Logistics **(connected with SAP)**
- Tank Inventory 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
- Meter Management PLC's
  - ControlLogic, SmartView
- Meters/Gauges
  - SmartRadar FlexLine, ABB, Honeywell VIT, Enraf 854 ATG Servo Advanced Tank Level Gauge

Tank Inventory Systems (Honeywell Enraf)



Tank Inventory Systems (Emerson TankMaster)



TankMaster distributes essential inventory tank gauging data.

Tank Inventory Systems (Emerson TankMaster)

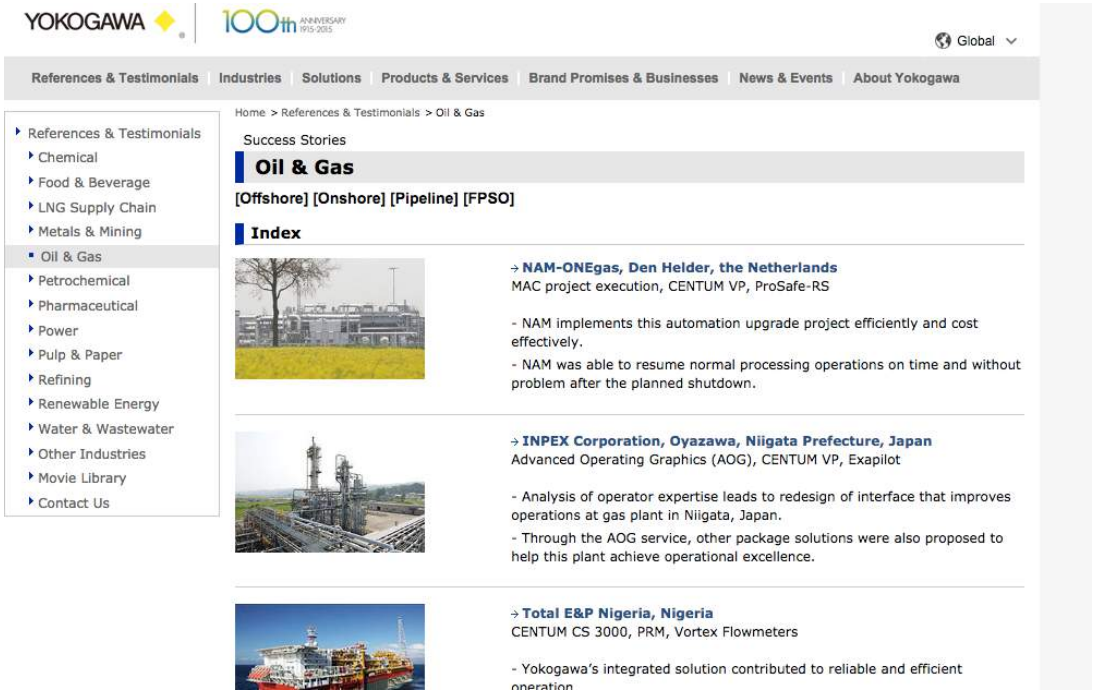
- Management console Emerson Rosemount TankMaster WinOpi
- View and **control**!
- Control commands
  - To change any alarm (Level, Temperature, Pressure)
  - To send management commands servo tanks (Freeze, Lock)

REFINERY

- Risks
  - Plant Sabotage/Shutdown, Equipment damage, Product Quality, Production Disruption, Compliance violation, Safety violation
- Oil refinery, is an industrial process plant where crude oil is processed and refined into more useful products
- Product examples: Gasoline, propane, jet fuel, heating oil, diesel fuel, kerosene, LPG, and petrochemicals
- Oil refineries are typically large, sprawling industrial complexes with extensive piping running throughout, carrying streams of fluids between large chemical processing units.
- Oil refineries have much in common with chemical plants
- **Technicians in a central control room can fine-tune refinery operations to produce the desired mix of products**

How can an attacker get to know what victim uses?

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



Enterprise Applications in Oil and Gas

Enterprise usage: Business Applications

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

Enterprise usage: Business Applications

70 million barrels per day *of oil are produced by companies using SAP solutions*

(75% of total Oil production)

What can happen

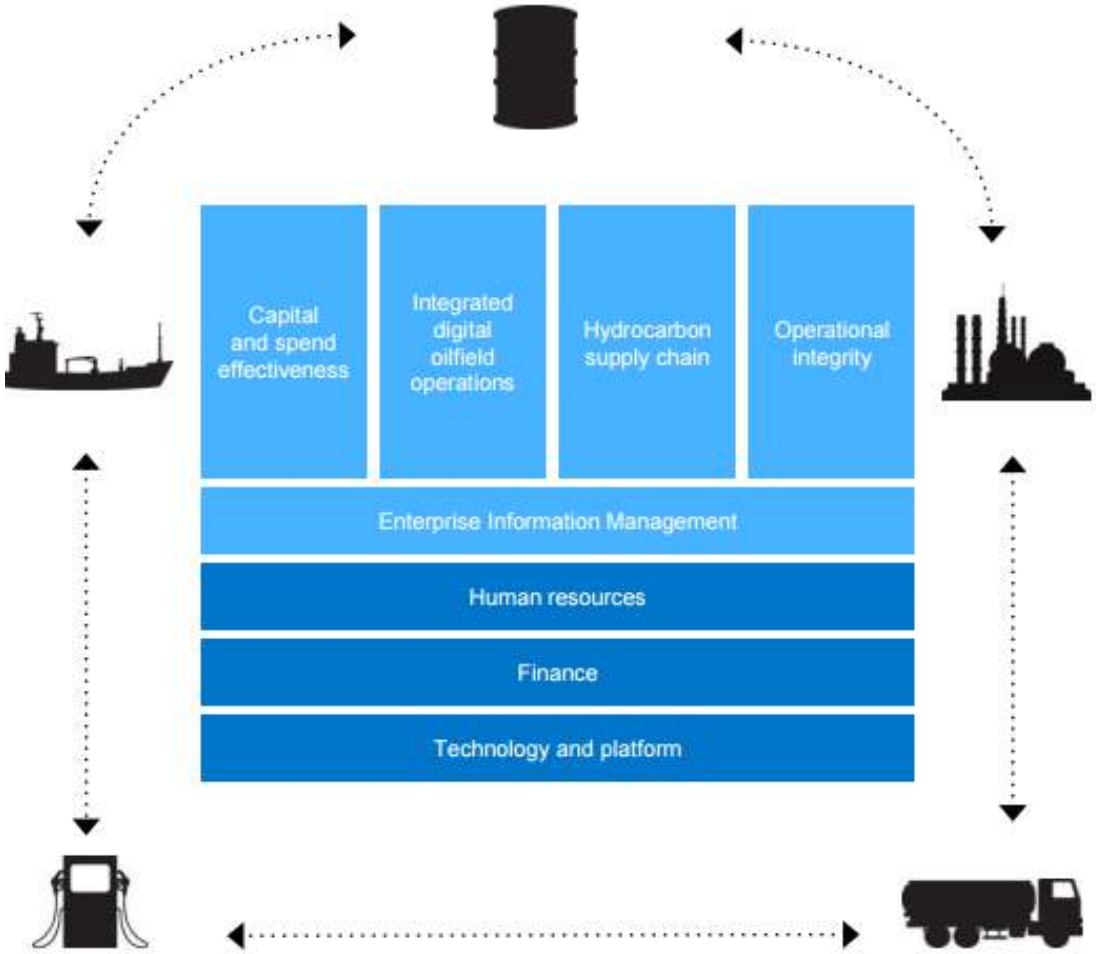
- **Espionage**
  - Theft of Financial Information
  - Trade Secret theft
  - Supplier and Customer lists theft
  - HR data theft
  - Other Corporate Data theft
- **Sabotage**
  - Denial of service
  - Modification of financial statements
  - **Access to Operations Technology network**
- **Fraud**
 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

SAP in Oil and Gas

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.*

SAP in Oil and Gas



SAP in Oil and Gas

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	

SAP In Oil and Gas: Capital and Spend Effectiveness

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

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
- SAP xMII

**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 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)
- SAP HANA

SAP In Oil and Gas: Operational Integrity

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

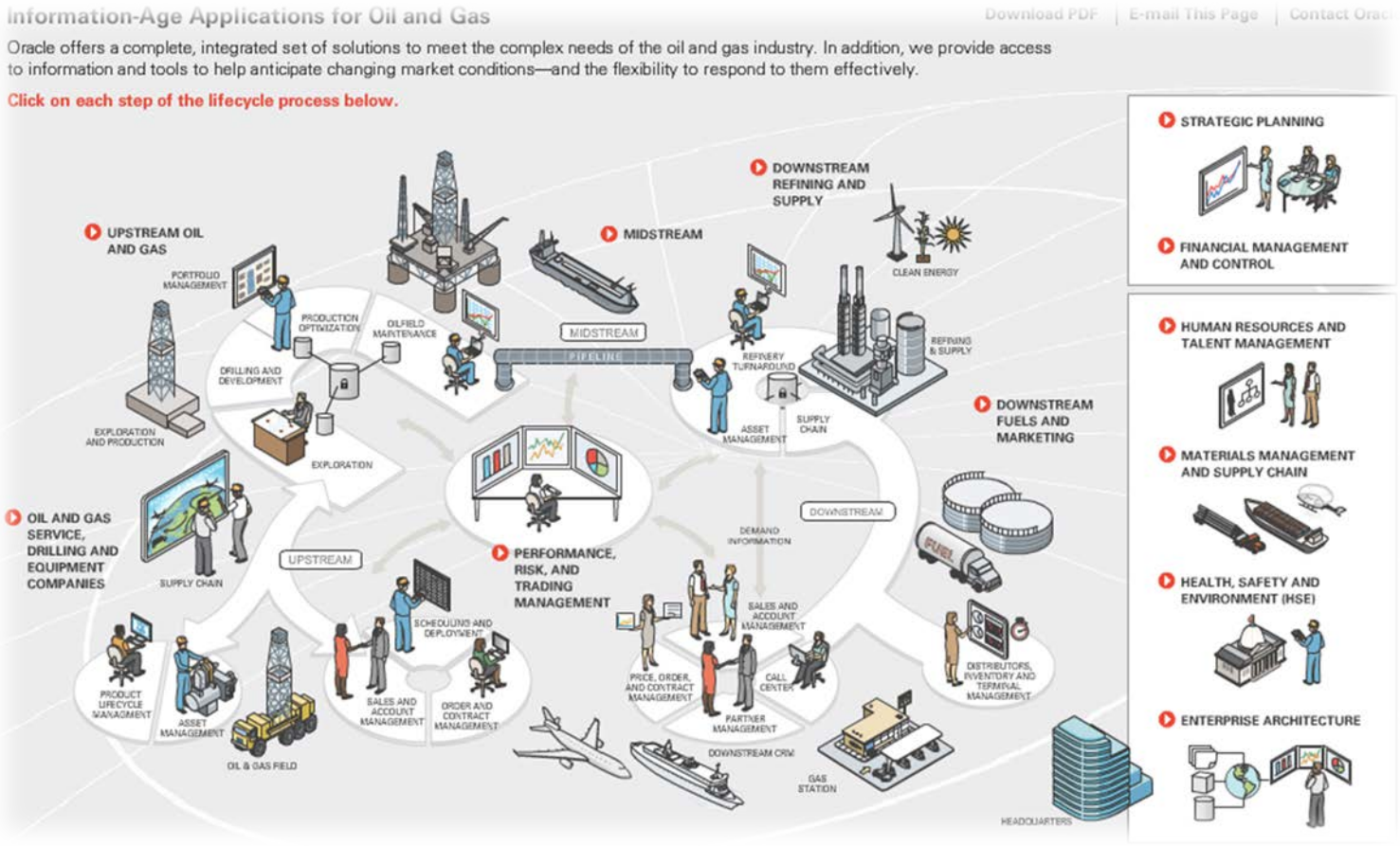
Risks:

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

Applications:

- SAP EAS/PM (Asset Management)

Oracle in Oil and Gas

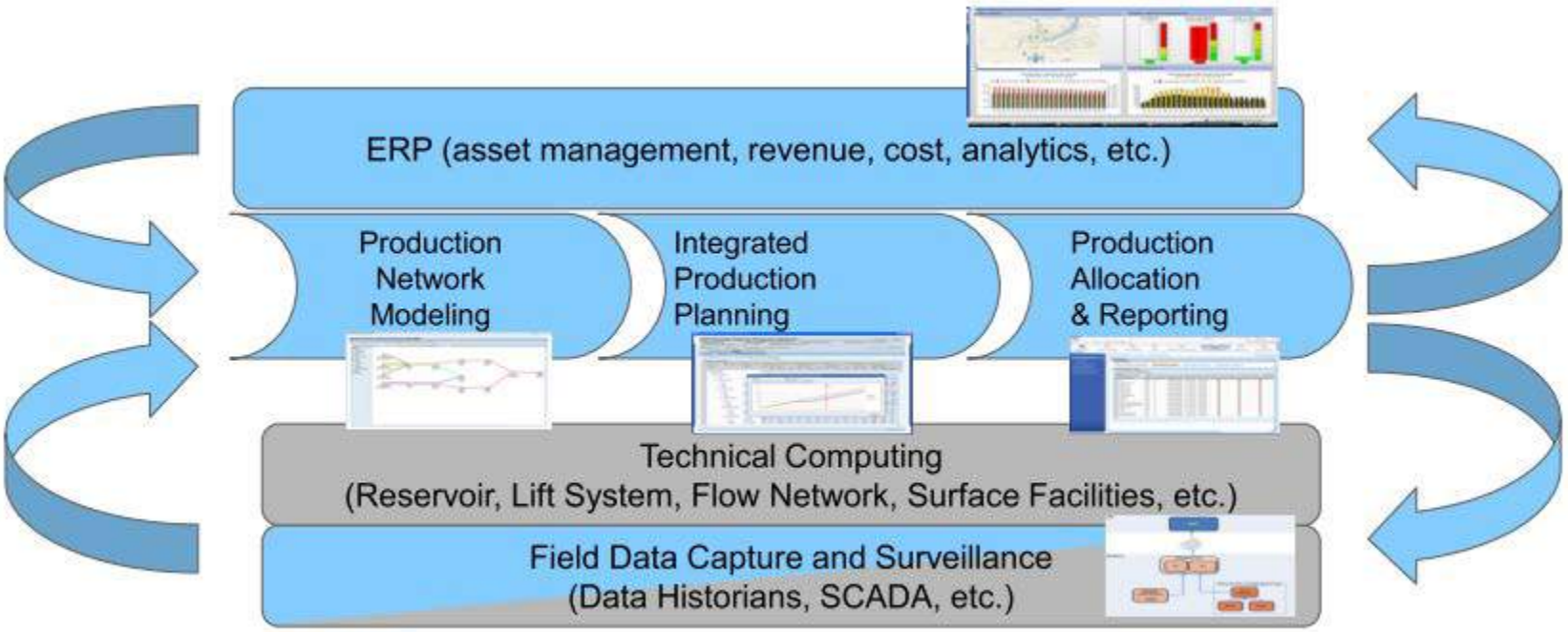


http://www.oracle.com/ocom/groups/public/@ocom/documents/webcontent/oil-gas.html

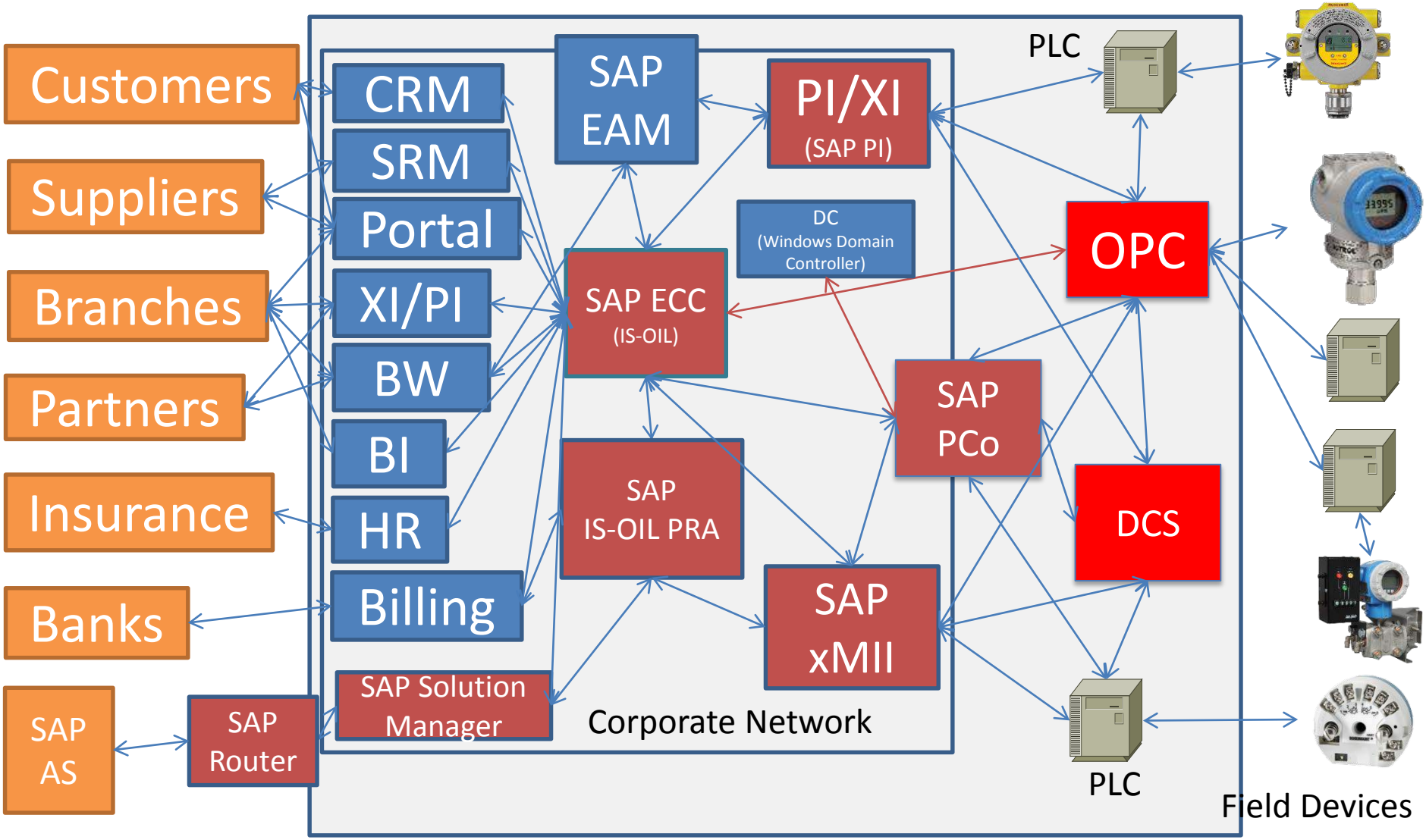
Enterprise applications VS Oil And Gas processes

- Enterprise project portfolio management <- Exploration
  - SAP PPM, Oracle Primavera, MS Project, MS SharePoint
- Asset Lifecycle Management <- Refinery, Separation, etc.
  - SAP EAM (+AssetWise APM), Oracle EAM, Avantis, IBM Maximo
  - Connect with: OSIsoft® PI System, AspenTech® IP21, Honeywell® PHD
- LIMS <- Refinery, Separation
  - Custom app based on Oracle DBMS
  - Connect with OSIsoft PI
- Tank Master Data <- Tank Inventory
  - SAP IS-OIL-TAS, Aspentech
- Production Accounting System (PAS) <- Fiscal Metering
  - SAP IS-OIL-PRA

IT/OT connection looks like this



Or like this


Customers
Suppliers
Branches
Partners
Insurance
Banks
SAP AS
SAP Router
CRM
SRM
Portal
XI/PI
BW
BI
HR
Billing
SAP Solution Manager
SAP EAM
PI/XI (SAP PI)
DC (Windows Domain Controller)
SAP ECC (IS-OIL)
SAP IS-OIL PRA
SAP xMII
SAP PCo
OPC
DCS
PLC
PLC
Corporate Network
Field Devices

Attacking Oil and Gas companies

From the Internet to CORP

Stage 1 (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-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 in the Internet
  - http://erpscan.com/wp-content/uploads/publications/SAP-Security-Attacking-SAP-clients.pdf

From Corp to ERP

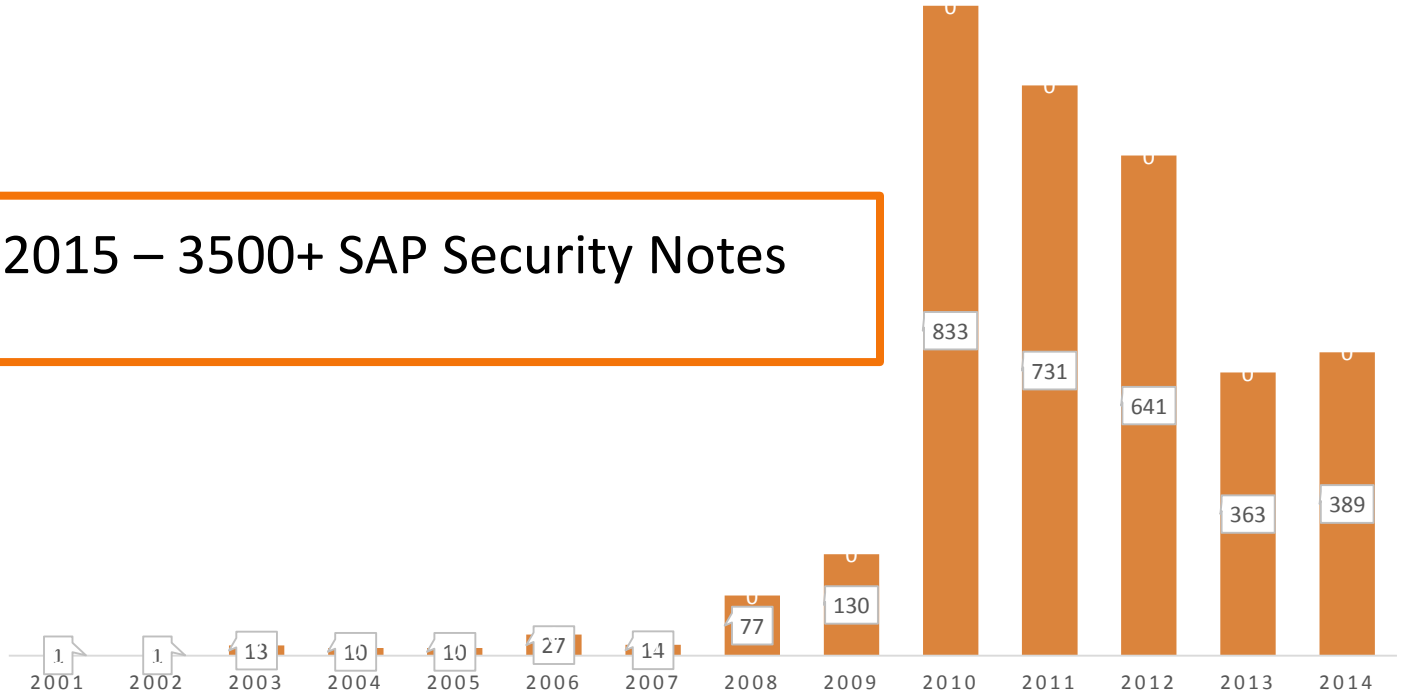
Stage 2 (From Internal Network to ERP)

Numerous ways how an ERP system such as SAP can be compromised:

- Vulnerabilities
- Misconfigurations
- Unnecessary privileges
- Custom code issues

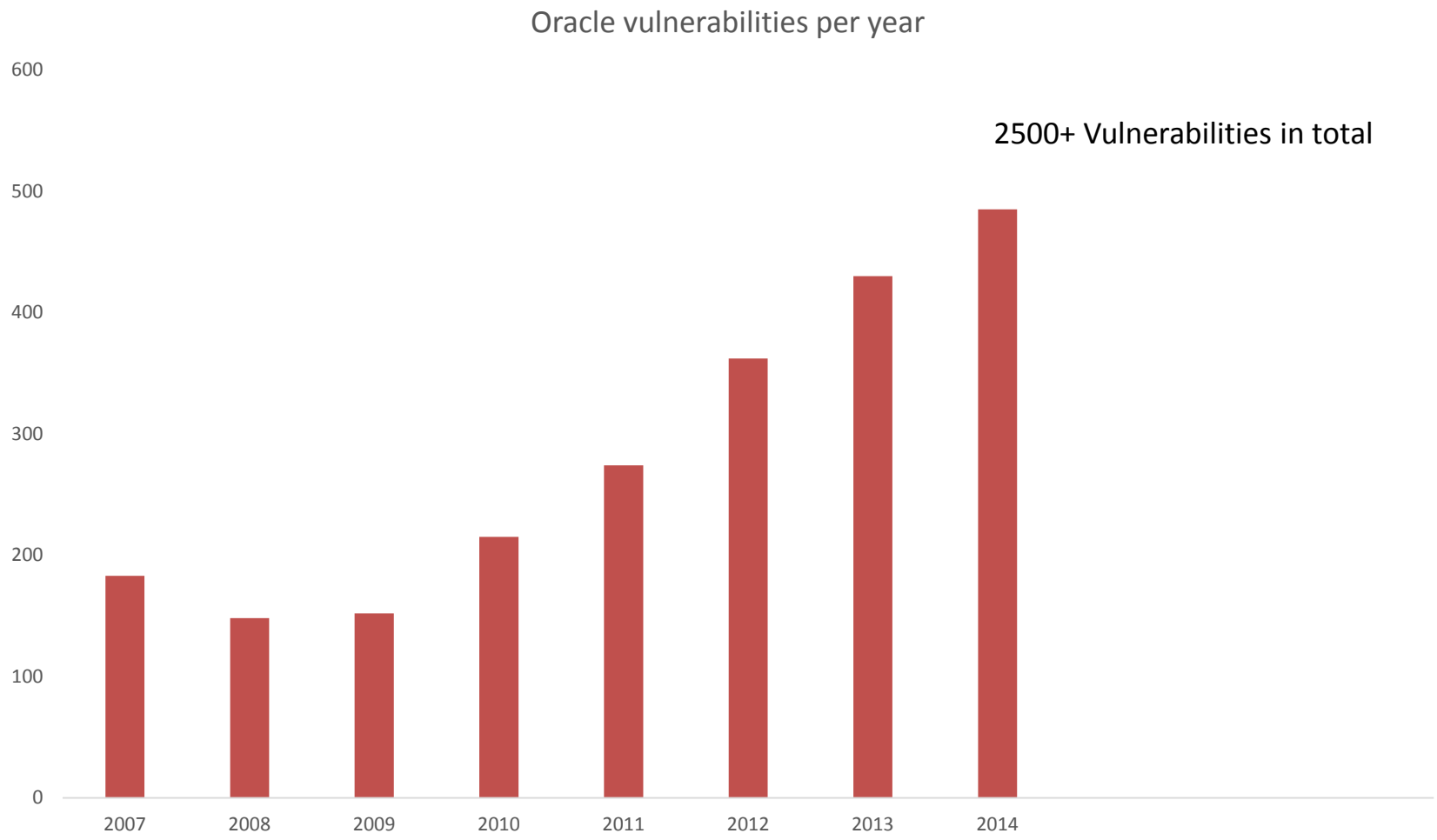
Stage 2 (Vulnerabilities in SAP Products)

By October 2015 – 3500+ SAP Security Notes



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

Stage 2 (Vulnerabilities in Oracle products)



Stage 2 (Misconfigurations in SAP)

- ~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 solutions…….)

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

Stage 2 (Custom code issues)

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

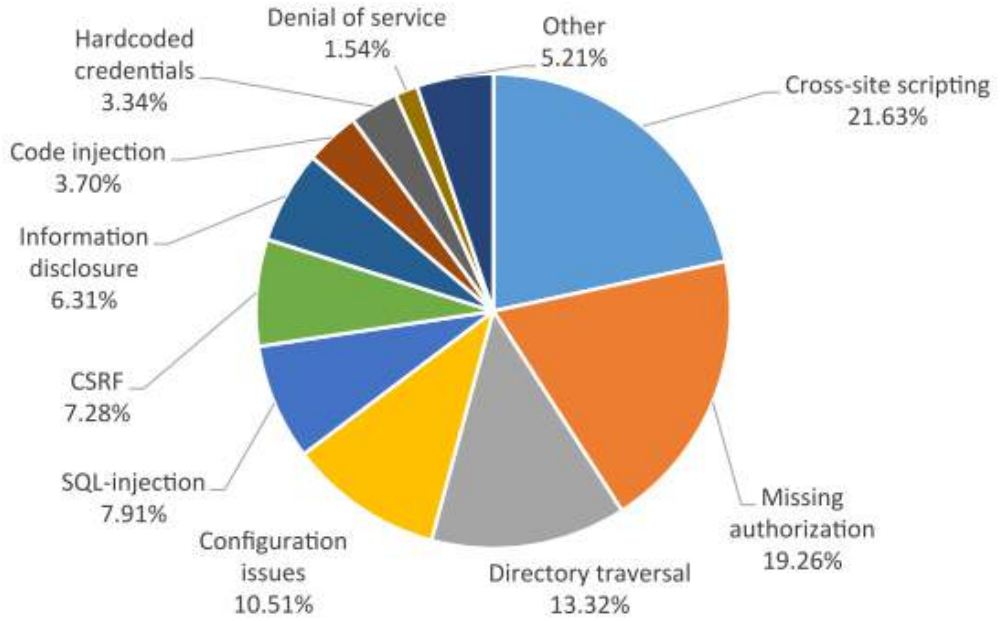


Figure 3.4-1 TOP-10 SAP Security Vulnerabilites, sorted by type

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

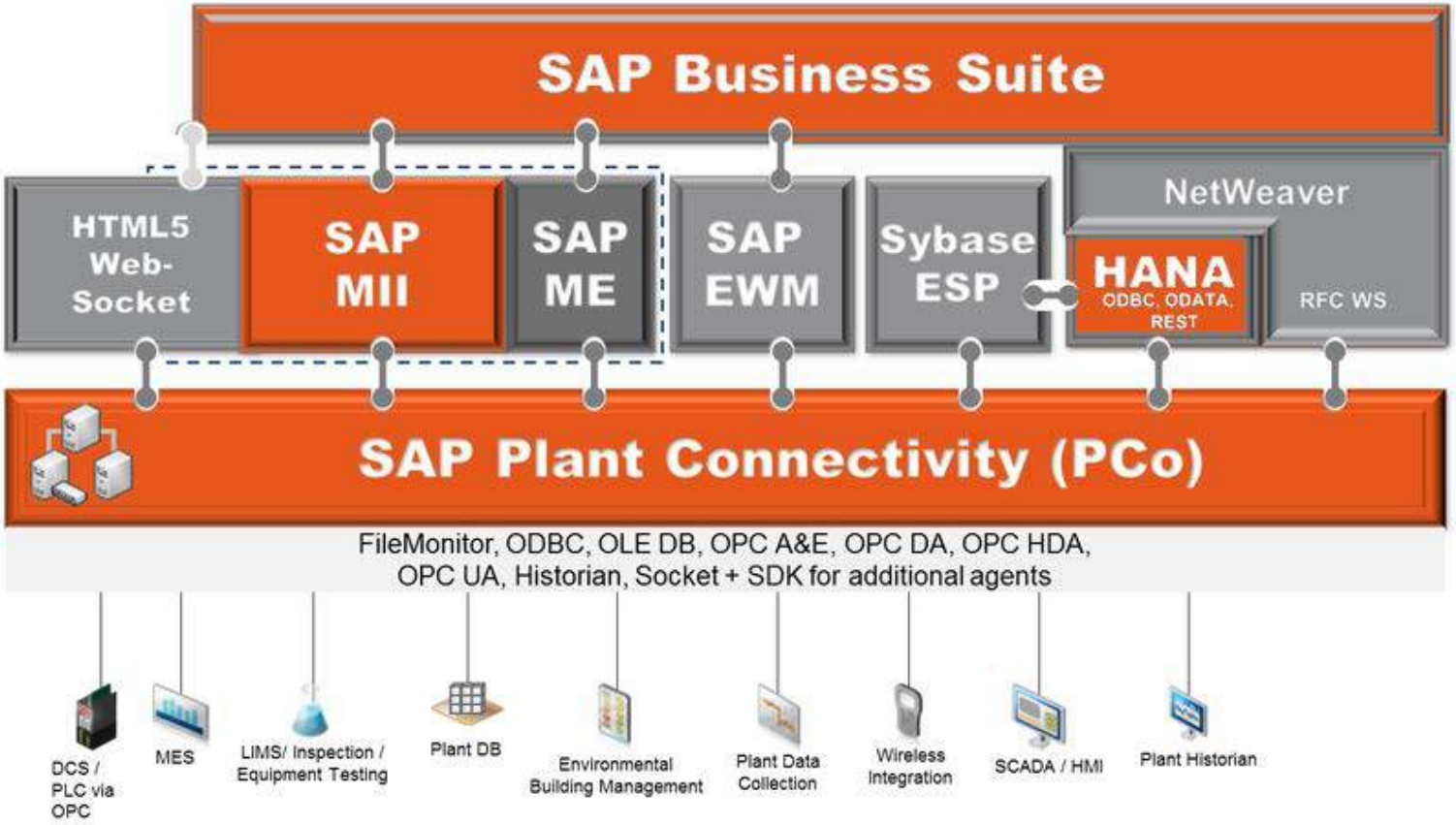
Stage 2 (Unnecessary privileges)

Critical privileges and SoD issues

- For example: Create vendor + Approve payment order
- 500k potential conflicts in typical company

From ERP to OT

Stage 3 (From SAP to Plant)



Stage 3 (From SAP to Plant)

- **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) -> OsiSoft PI -> DCS -> PLC-> Meter
- **Oracle EAM -> OsiSoft PI -> DCS -> PLC-> Meter**
- Domain Controller -> SAP PCo -> PLC -> Meter
- Shared SSH keys
- Similar passwords
- Improper firewall configuration

Stage 3 (From SAP to Plant)

Finally, we need to find a way to hack

- **Oracle EAM**
- **SAP HANA**
- **SAP xMII**
- **SAP PCo**

Stage 3 (Hacking Oracle EAM)

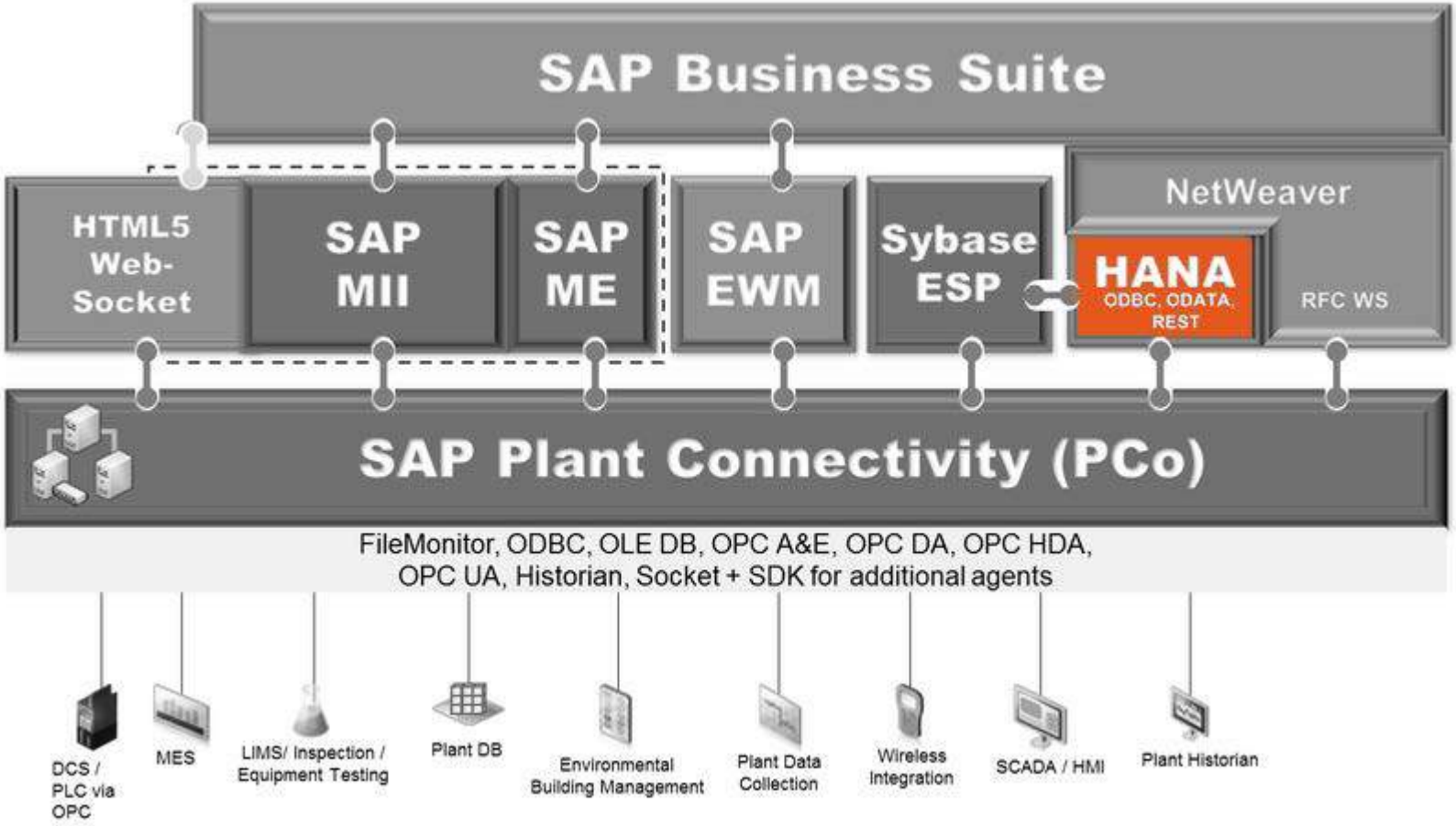
- Oracle Enterprise Asset Management is an application based on Oracle E-Business Suite platform.
- Thus, every vulnerability that can be used to get unauthorized access to Oracle EBS can be used to break into Oracle EAM system.

Attack Surface (Oracle EAM Security):

- ERPScan's experts have recently disclosed details of 6 vulnerabilities in Oracle E-Business Suite.
  - XSS Vulnerability,
  - SQL Injection vulnerability,
  - XXE Injection Vulnerabilities, ([1], [2])
  - User Enumeration vulnerability.

http://erpscan.com/press-center/press-release/erpscan-took-a-closer-look-at-oracle-ebs-security-6-vulnerabilities-patched-in-recent-update/

Stage 3 (Hacking SAP HANA)



Stage 3 (Hacking SAP HANA)

- SAP HANA collects the most critical data from Plant for analytics
- It is a database used by many SAP and non-SAP applications
- Some of them (RoltaOneview) also store critical data to analyze
- Administrators rarely read SAP HANA Security guides

Attack Surface (SAP HANA Security):

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

Stage 3 (Hacking SAP HANA)

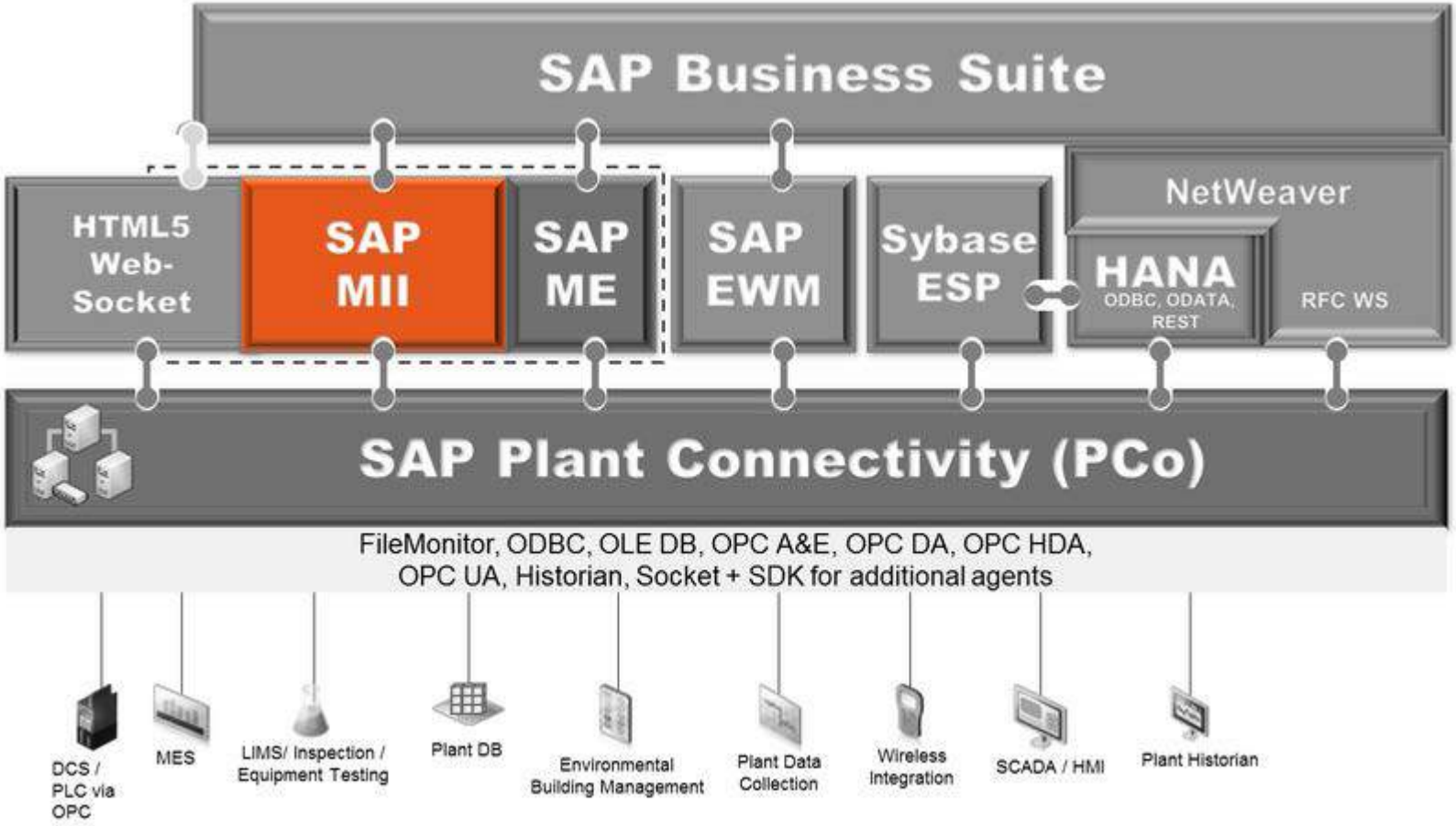
- **[ERPSCAN-15-024] SAP HANA hdbindexserver – Memory corruption**
- An anonymous attacker can use a special HTTP request to corrupt SAP HANA index server memory.
- An attacker can use vulnerability to execute commands remotely without authorization, under the privileges of the service that executes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

Stage 3 (Hacking SAP HANA)

Correction

SAP Note 2197428

Stage 3 (Hacking SAP xMII)



Stage 3 (Hacking SAP xMII)

Some systems should be connected at least on the network layer

Attack Surface (SAP xMII Security):

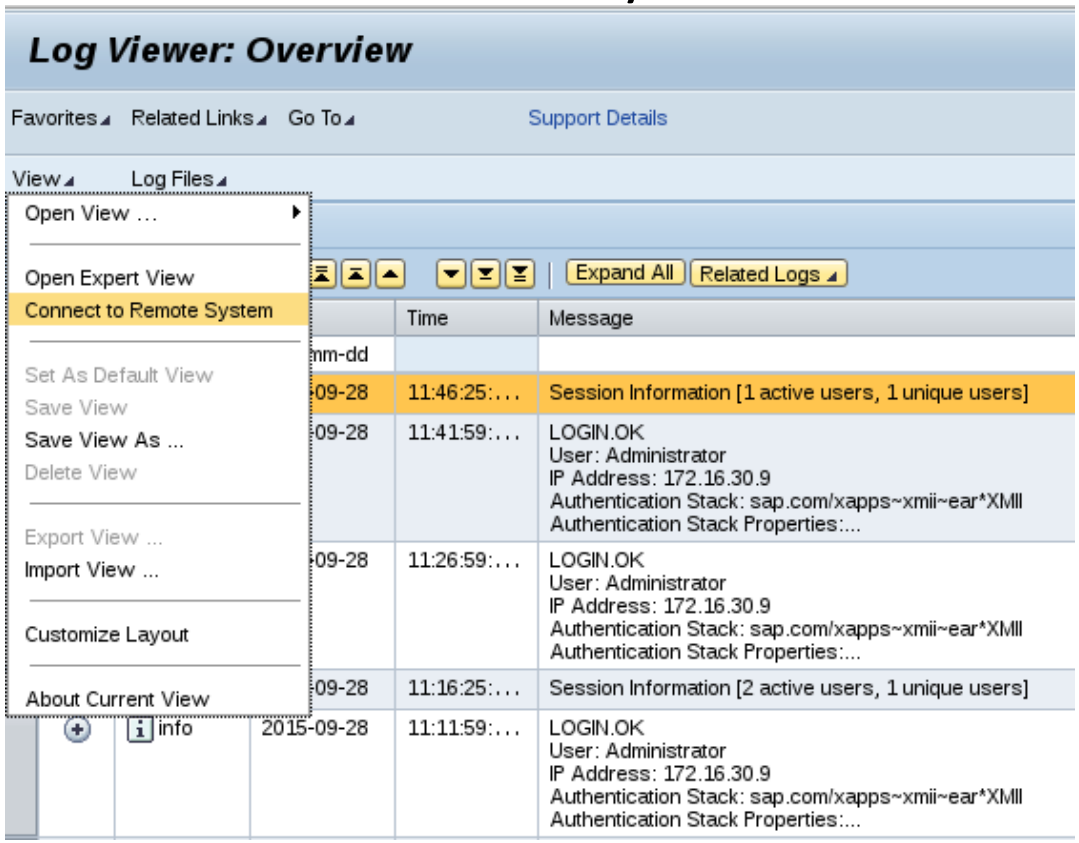
- SAP RFC links from ERP to xMII
- **NetWeaver J2EE Platform vulnerabilities (core of xMII)**
- Direct SAP xMII vulnerabilities (XXE)
- Database links to xMII
- Shared SSH keys
- Similar passwords
- Others

Stage 3 (SAP SAP xMII overview)

- MII: Manufacturing Integration and Intelligence
- Connects manufacturing with enterprise business processes, provides 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~mii~ears` is the main application with several endpoints accessible at http://server:50000/XMII
- Has some vulnerabilities (Blind SQLi/XXE) [can't disclose details]

Stage 3 (Getting OS access to SAP xMII)

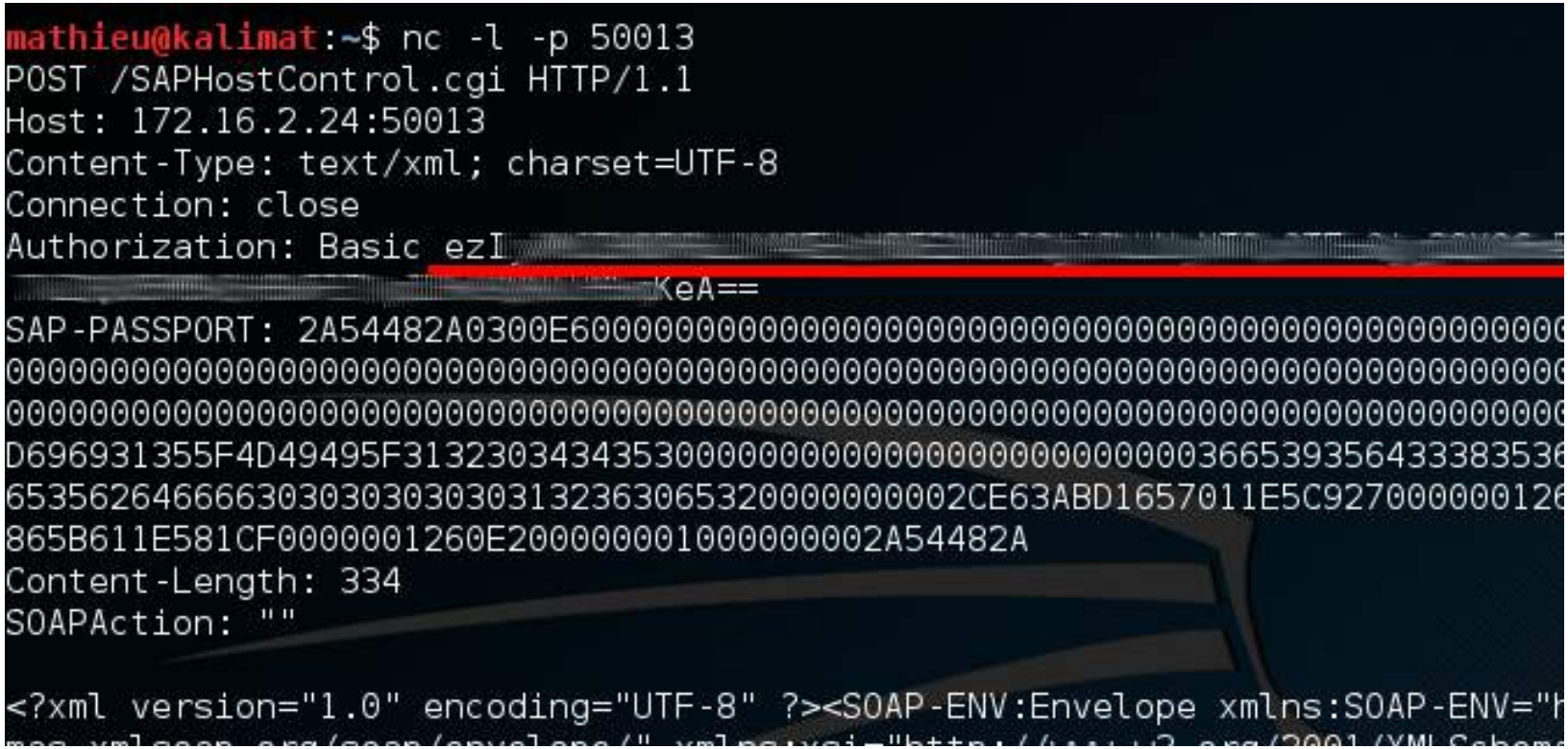
- We have Admin access, but how to execute OS commands?
- In «Log viewer» we chose «Connect to Remote System»



Stage 3 (Getting OS access to SAP xMII)

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

Stage 3 (Getting OS access to SAP xMII)

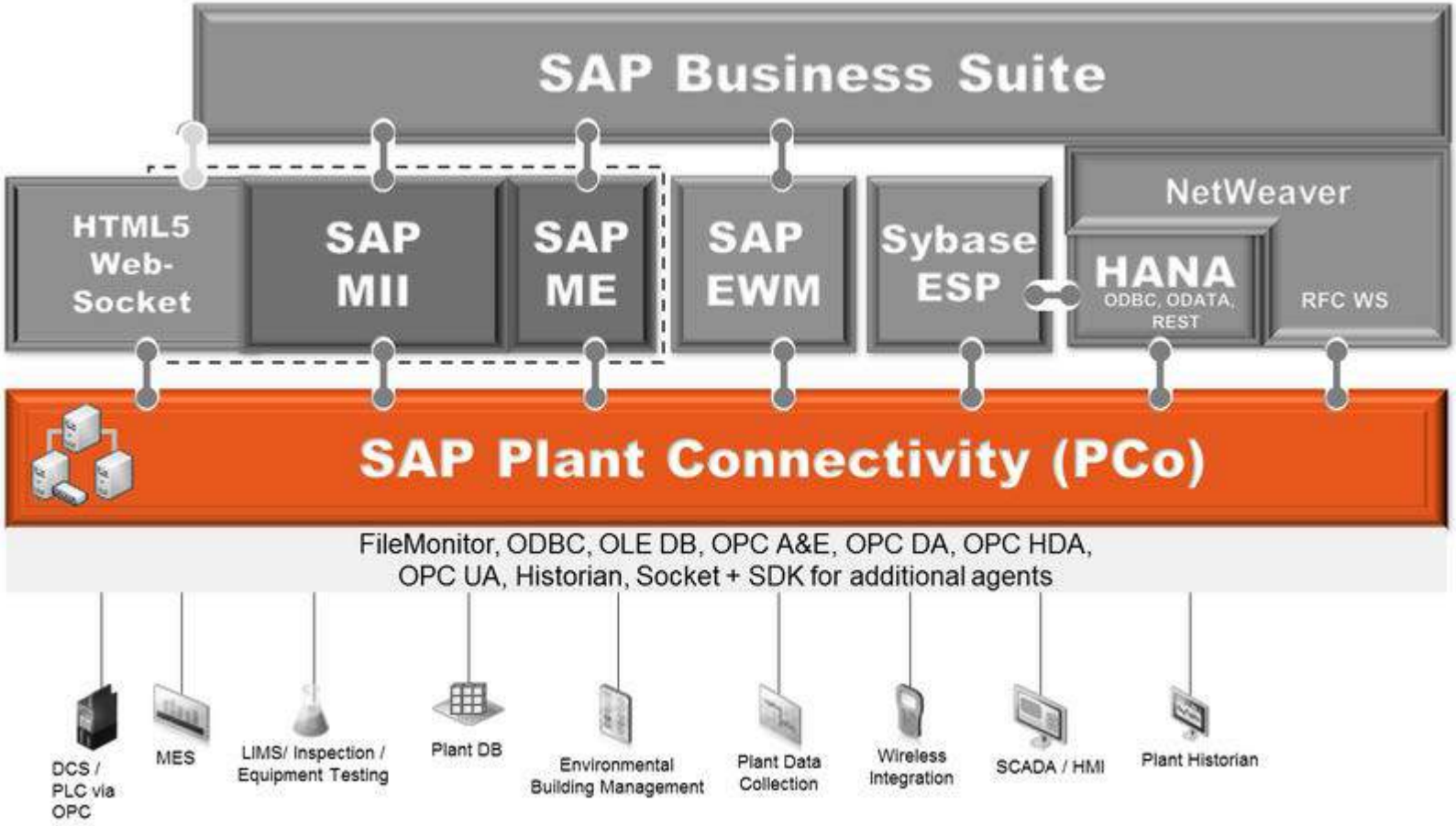


Request contains Basic Authentication header
We decode it as user « {221….} » and password x**********x
The password is random and lives max. the JVM lifetime

Stage 3 (Getting OS access to SAP xMII)

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

Hacking SAP Plan Connectivity



Hacking SAP Plan Connectivity

SAP Plant Connectivity (PCo) usually stays between SAP xMII and Critical device

Attack surface (SAP Plant Connectivity Security):

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

SAP PCo overview

- 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

Hacking SAP PCo

- 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?
- Inside the SecureStorage
- But…

Hacking SAP PCo (lower encryption)

Hacking SAP PCo (now encryption is Base64)

Hacking SAP PCo (now encryption is Base64)

Correction

SAP Note 2240274

Stage 3 (Hacking PCo)

- 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

Stage 3 (SAP PCo – post-exploitation)

- 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
    - Fuzzing (Kill agent + mem leak)
  - Exploitation of the source via this channel?

Correction

SAP Note 2238619

Advisory

http://erpscan.com/press-center/blog/sap-security-notes-november-2015-review

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

Stage 4 (Access to DCS/OPC/SCADA)

- SAP Plant Connectivity interacts with DCS/OPC
  - **On the same workstation**
    - **Required when configuring some DCS/SCADA systems**
  - **On the same network**
    - Example: 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) Planning to send it to vendor
- DCS/SCADA can control PLC
  - **Attack PLC using access to DCS/SCADA**
  - **Attack PLC via PLC vulnerabilities**
    - Example: ABB AC500
      - ICSA-12-320-01 : ABB AC500 PLC Webserver CoDeSys Vulnerability

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 to 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.

Interface between SAP and OSI - PI

This question has been **Answered.**

Team,

Appreciate your response for a query from a customer. Find below

Kindly help us to get some more details from SAP about the connectivity between OSI-PI system and SAP (PP,EHSM and QM).

Because, we might use only for one way communication (pull) the data from OSI-PI to get plant information to update our SAP –ECC for informative purpose of production reports and EHS.

Queries:

Recommend that you use PCo amd MII to integrate to ECC. MII has JCO and BAPI connectors for ECC as well as the capablilty to implement Listeners to receive IDOC from ECC. MII has additonal capabilities such as the Plant Information Catalog that will be very beneficial in defining historian data and providing business context around it.

PCo has a native OSP PI connector as well as MII connectors that can execute MII transactions directly; the transactions can then execute JCO and BAPI to ECC.

PCo can connect to Honeywell PHD using the PCo OPC HDA connector. (The Honeywell historian OPC server will need to be installed and activated, preferably on the PCo server.) PCo also has connectors for TCP Socket, OPC DA, OPC UA, OPC AE, ODBC, OLEDB, FileMonitor, and additional native historian connectors (Aspentech IP21, GE Proficy, CiTectSCADA).

DEMO

Oil and Gas attack vectors

Oil market fraud attack:

- 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.
- Imagine what would happen if a cyber criminal uploads a malware that dynamically changes oil stock figures for all Oil and Gas companies where SAP is implemented.
- In case of successful attack, cyber criminals can control about 75% of total Oil production.
- Attackers will be able to deliberately understate data about Oil in stocks of affected companies to increase Oil prices, or vice versa.

Attack vectors

Plant equipment sabotage attack

- 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 the talk. The easiest way to do so is to hack an SAP's or Oracle's Asset Management solution. Another system which can be under attack is Rolta OneView.

Plant Destruction attack

- Burner Management Systems (BMS) and other critical systems are used in numerous processes including Separation and Refinery.
- Some of these 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 xMII;
- With access to BMS systems, hackers can perform physical attacks.

How does one go about securing it?

ERP Security

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

ERP Security

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

Takeaways

- Researchers - now you know where to start from, Oil and Gas security is a small universe.
- Pentersters - 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 first.

About

a.polyakov@erpscan.com

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
info@erpscan.com

Products

- ERPScan Security Scanner for SAP
- ERPScan Security Monitoring Suite for SAP
- ERPScan Security Monitoring Suite for Oracle PeopleSoft

Services

- SAP Vulnerability Assessment
- SAP Security Trainings
- SAP Security Audit
- SAP Custom code security review
- SAP Penetration testing