Rig Security in the IOT World

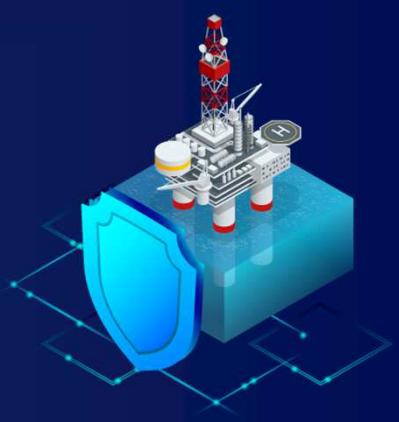
Jon Curtis – Chairman Emeritus Petrolink International Ltd.

10/07/2019

Protecting Rig Data Assets from Cyber Threats

- A growing trend in our industry is to move from back-office processing to data fed analysis and decision making at the edge where the bit meets geology. In this new world of edge-based analytics, we need to balance this thirst for data with the need to protect data asset and security from digital threats.

  This webinar discusses possible techniques for connecting, converting and standardizing data for analytical use and also protecting the corporate network including physical and network barriers to isolate the rig while still allowing for authorized interactivity

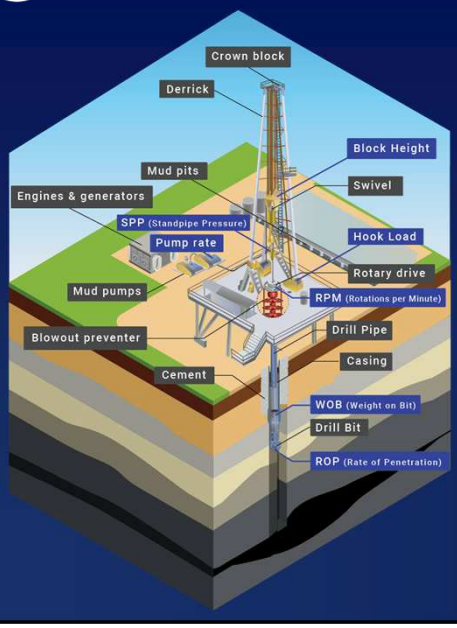


Industrial Internet of Things (IIoT)

- "The connection of digitally networked sensors and sensor-based data to visualisation and analytics environments hosted in the cloud or on premises. IIoT enriches existing data ecosystems to enhance decision support for actions influencing control, design and service in industrial operations"
- Cisco: "By 2020 50 billion devices will be deployed and active"
- But on Drilling Rigs….. ?

Source: https://www.instrumentation.co.za/55128n

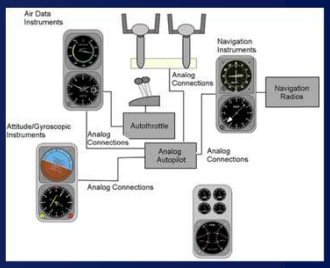
Fundamental Drill Rig Instruments



- Block Height
- Hook Load
- Rotations per Minute
- Flow Rates
- Stand-Pipe Pressure
- Blow Out Preventer
- Engines
- ~ 20 Surface Sensors

Fundamental Flight Instruments

- Airspeed Indicator
- Attitude Indicator
- Altimeter
- Vertical Speed Indicator
- Heading Indicator
- Turn Coordinator

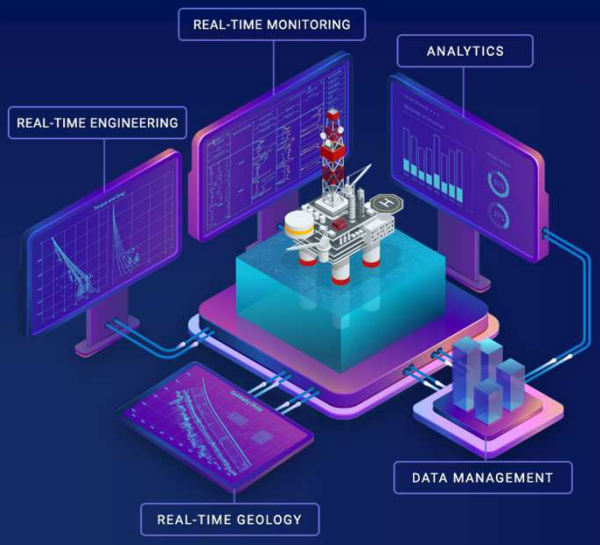


How many Sensors in Avionics now ?

- Airbus A350 – 6000 Sensors which generate 2.5 tB / day
- Airbus A380 will have 10,000 Sensors in each Wing (Year 2020), and generate 7.5tB / day

Source: Data Science Central Online

Digital Ecosystem around a Rig

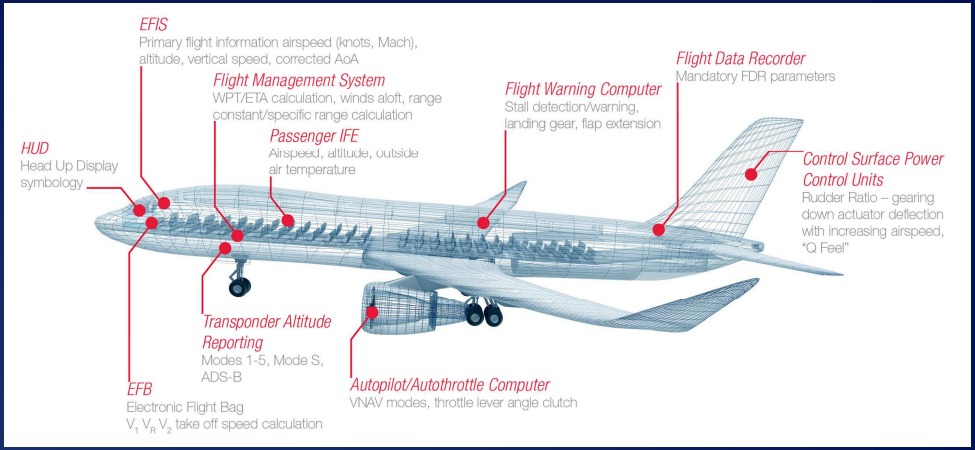


Digital Ecosystem around an Aeroplane

- Aeroplanes are so connected, the even the public can monitor the vitals.
- Each airline and aeroplane manufacturer has their own monitoring system and centre and tracks even more data and focuses on matters such as safety and optimization.

Source: Image – Flightradar24

Digital Ecosystem on the Aeroplane



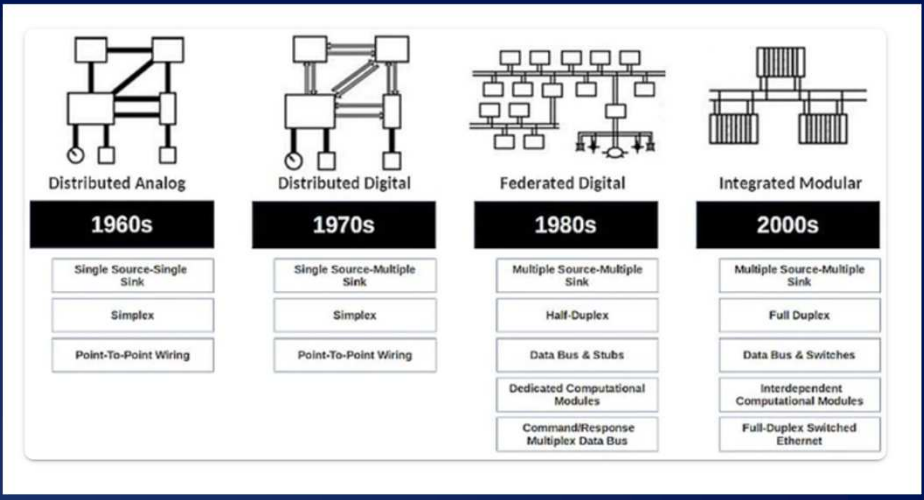
Source: **Image –Aviation International.**

Digital Ecosystem on the Rig : X

Where is the Roadblock then ?

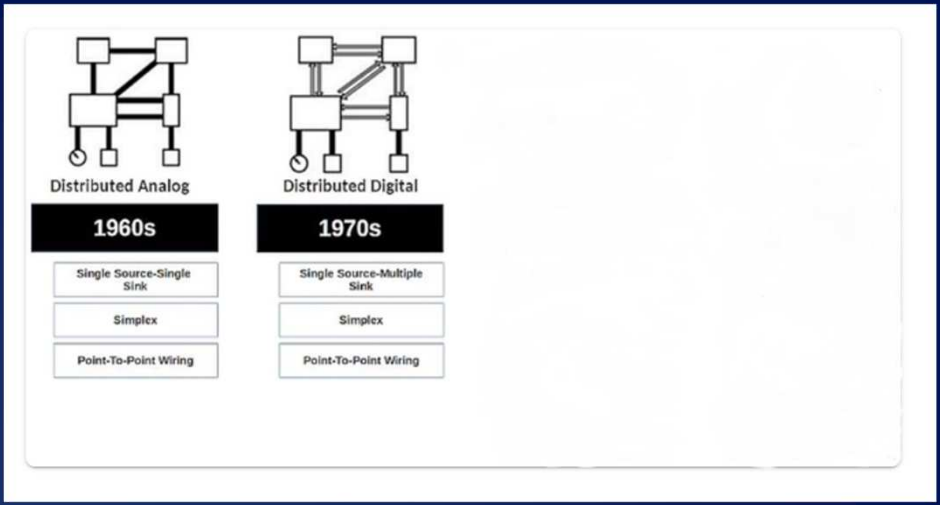
- The Aircraft has complete interconnectivity between all component parts even though they have been manufactured by different companies
- The Oil Rig has a Drilling Data Acquisition System owned or leased by the Rig Contractor but typically other equipment manufactured by third parties such as the BOP is NOT CONNECTED.
- Initial efforts were to interconnect equipment used OPC Tags
- Data Transfer standards switched to WITS, then WITSML
- Rig Networks are contractor specific and there is no IT resource to manage interconnectivity – only a Rig Electrician in most cases
- Vested Interests prevent collaborations which would have value to all parties

Timeline of Avionics Architectures



Source: https://www.intelligent-aerospace.com/commercial/article/16544804/milstd1553b-in-avionics-where-data-networking-has-been-and-where-its-going

Timeline of (most) Oil Rig Architectures



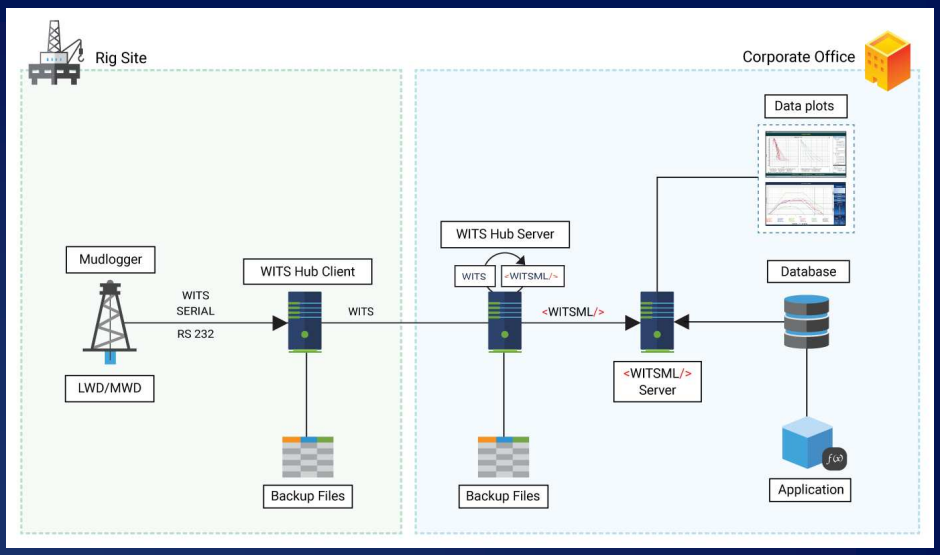
Source: https://www.intelligent-aerospace.com/commercial/article/16544804/milstd1553b-in-avionics-where-data-networking-has-been-and-where-its-going

Data Standards – WITS, WITSML, OPC ??

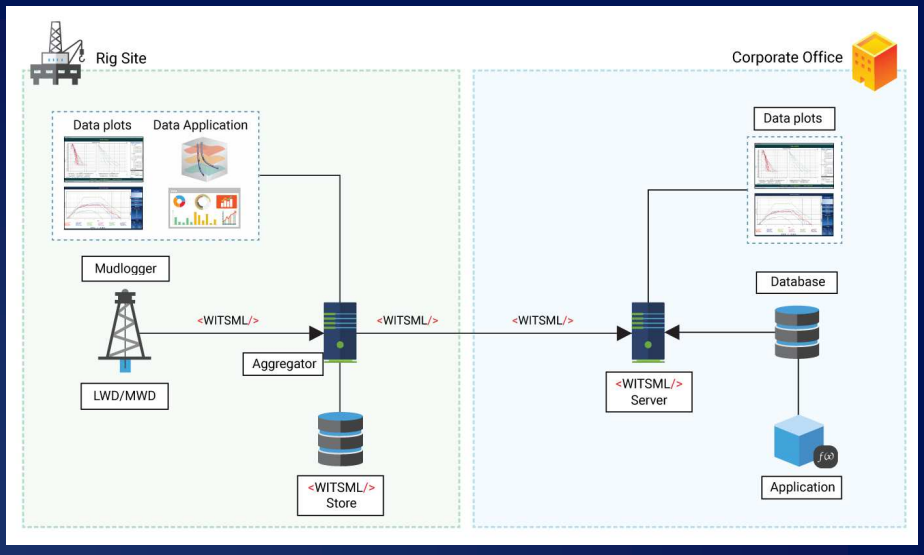
- WITS data is ASCII and therefore cannot carry Malware
- WITS has been largely replaced by WITSML and the trend is continuing
- WITSML is based on XML which is particularly vulnerable to Malware Attacks
- "The flexibility of XML has resulted in its widespread usage, including within Microsoft Office documents and SOAP messages. However XML Documents have many security vulnerabilities that can be targeted by different types of attacks, such as file retrieval, server side request forgery, port scanning or brute force attacks"
- WITSML is managed by Energistics which provides guidelines for the creation of WITSML Client and Server implementation, but these are not well defined

Source: CNBC Online

WITS data from the Wellsite



WITSML data from the Wellsite



Cyber Threats in the Oil & Gas Industry

An integrated approach to combat cyber risk: Securing industrial operations in oil and gas

The oil and gas industry is making its way to the next level of digital evolution, embracing and integrating robotics, digitization, and the Internet of Things (IoT) into the operational environment. This has led to new opportunities to improve productivity and drive down costs. However, the convergence of operational and business systems has also opened up the company to a whole new array of cyber risk.

This report shares the insight gained from our extensive field experience, including lessons learned in helping oil and gas companies to go beyond safety in securing their ICS. This report examines how cyber threats impact the oil and gas value chain.

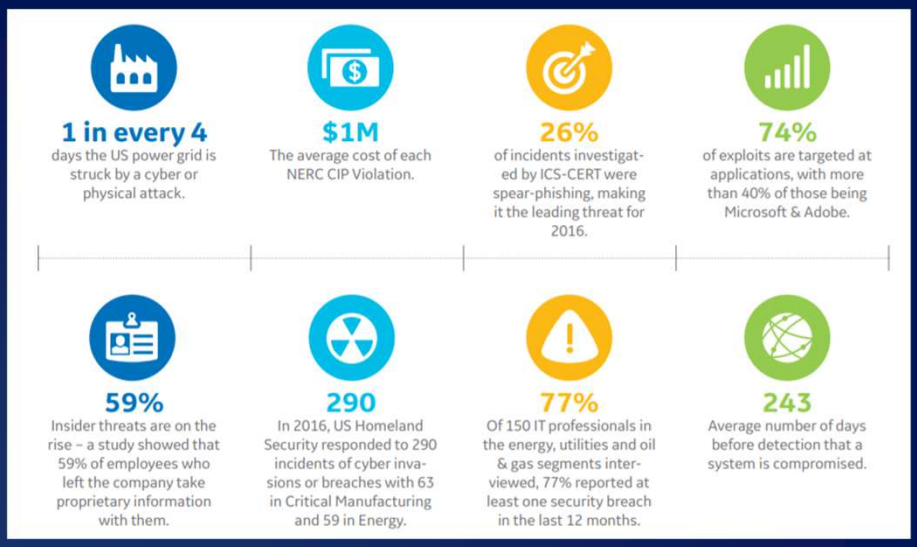
Source: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/intergrated-approach-combat-cyber-risk-oil-gas.pdf

The Oil & Gas Industry is a Cyber Target

For years, cyber attackers have targeted O&G companies, with attacks growing in frequency, sophistication, and impact as the industry employs ever more connected technology. The strategic and financial value of these companies make them extremely attractive targets, both to cyber criminals and state agencies.

Previously the industry has been able to rely on remote operations and complex data structures to provide some level of natural defence, but this is no longer the case. The upstream oil and gas industry is fast evolving; factors such as automation; digitalization and IoT technology are rapidly integrating to form a highly complex operational ecosystem. However, the industry's march toward interconnectedness has outpaced its progress on cyber security making it a prime target for cyber-attacks...and these attacks could have cataclysmic consequences. If a cyber attacker were to manipulate the cement slurry data coming out of an offshore development well, black out monitors' live views of offshore drilling, or delay the well-flow data required for blowout preventers to stop the eruption of fluids, the devastation could be staggering. "

Cyber Security by the Numbers



Source: https://www.bhge.com/system/files/2018-09/BHGE_Cybersecurity.pdf

How could Cyber threats be implemented ?

- XML Injection
- XSS/CDATA Injection
- Oversized Payloads or XML Bombs
- Recursive Payloads
- VRA Macros
- Javascript

```
<temperature>
   &lt;script&gt;malicious code&lt;/script&gt;
</temperature>
```

The above sample is an XML element named "temperature." Its content can be uploaded to a website, and the JavaScript code is run when a user opens the website.

Source: https://www.opswat.com/blog/depth-look-xml-document-attack-vectors

Ever Growing Threats

- Cyber attackers on O&G companies growing in frequency, sophistication and impact as the industry employs ever more connected technology.
- The strategic and financial value of our industry makes an extremely attractive target for cyber criminals and state agencies.
- Stuxnet, Night Dragon, Shamoon and NotPetya have conclusively proven that attacks are capable of infiltrating standard Cyber Security defences
- The rise of IoT and reliance on automation will present entirely new threats and significant extra risk
- We need an industry specific methodology that is secure, vigilant, resilient and capable of mitigating the emerging threats an increasingly interconnected infrastructure.

What is changing …..

- Historically remote operations and proprietary data structures provided basic natural defence. This is no longer the case.
- Automation; digitalization and IoT technology are rapidly integrating to form a highly complex operational ecosystem. This march toward interconnectedness has outpaced its progress on cyber security making it a prime target for cyber-attacks
- These attacks could have cataclysmic consequences

IOT on the Remote Rig Site ?

- Internet of Things (IoT) gives greater ability to create, communicate, aggregate, analyze and act upon the data.
- Enabled through sensor technology, communication networks and analytical and automated tools
- These stages are each highly vulnerable to security breaches in legacy industrial control systems and complex upstream ecosystems. Intelligent field devices that can self-process, analyze and act upon collected data closer at “the edge” have taken cyber risks into the front line of upstream operations. (a malicious hacker directly attack pumping systems, BOPs or other field equipment)

Cyber Threat Case Study: NotPetya

- Government State sponsored piece of malware targeting Ukraine
- Uses a highly sophisticated OS exploit (Mimikatz) combined with a security "backdoor" embedded in Windows by the National Security Agency (Eternal Blue) to infect and shut down entire corporate networks
- Whitehouse estimated damages in excess of $10 billion, with notable victims including Merck ($870,000,000), FedEx ($400,000,000) Saint-Gobain ($384,000,000), Maersk ($300,000,000), Mondelēz ($188,000,000) and Reckitt Benckiser ($129,000,000)
- Similar state sponsored attacks could be targeted directly at National Oil Companies and Super Majors

Source: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Cyber Threat Case Study: StuxNet

- Probably a State led attack on Iranian Nuclear Industrial Systems
- Breached “Industry Certification” protocols to enable the malware to inject itself across multiple platforms
- Able to traverse across multiple operating systems (Windows, Linux, Siemens) invisibly
- Specifically aimed to attack hardware through corruption of operating parameters past safe limits
- Physically destroyed equipment worth more than $100,000,000
- Shut down targeted facilities for months

O&G Worst case scenarios

Scenarios:

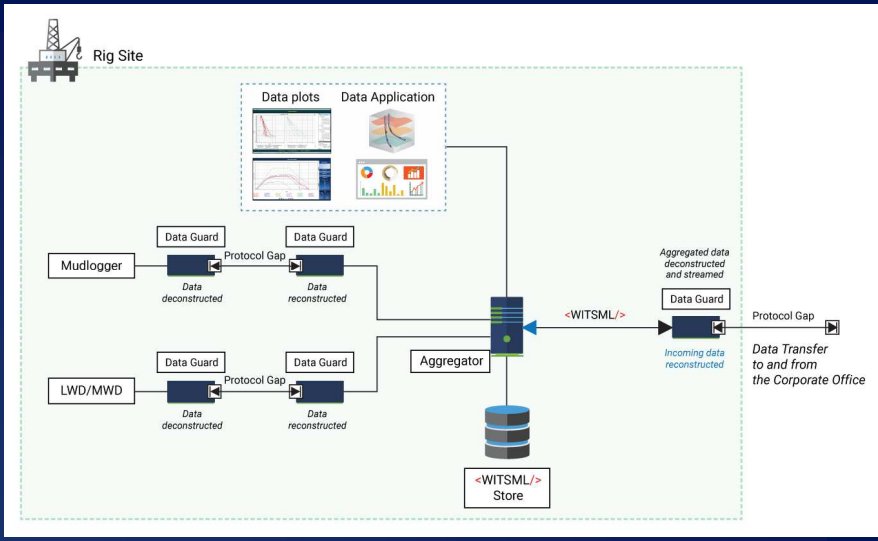
- Manipulate cement slurry data coming out of an offshore development well
- Shut down or manipulate telemetry data coming live from offshore wells
- Attack the oil extraction process by varying the motor speed and thermal capacity of an integrated sucker rod pump by altering speed commands sent from internal optimization controllers.
- delay the well-flow data required for blowout preventers to stop the eruption of fluids
- Directly target Industrial Control Systems to induce failure or malfunction

Potential Cost: Limitless (A deliberate Macondo)

Barriers to Attack

Secure Boot –Verifies the bootloader is trusted against PTT before it can load.
Trusted Boot – Analyses the signature of the Windows kernel before loading it, then verifies each of the components of the start-up process, including boot drivers, start-up files and anti-malware applications
Early-Launch Anti-Malware – Forces a malware check for all boot drivers and applications before they can be loaded by the system.
Application Control – Dedicated security hardware that allows only applications on an Administrator controlled approved list to run. This is tested using code integrity and certificate checks performed outside of the OS kernel, so even if Windows is compromised malware or malicious users cannot run untrusted software on the device.
Assigned Access – Restricts system users to only being able to launch the UniDAQ app.
Device Health Attestation – Forces the device to perform a health check based on sending encrypted boot logs to an independent verification server before it can access any other network resources.

Interconnectivity on the Rig : Protocol Gap Device



Protocol Gap

- Isolates Operator Network from the Wellsite Aggregator and thereby the Contractor Networks
- Isolates Contractor Networks from each other
- Deconstructs TCPIP Data and re-assembles it beyond the Protocol Gap
- Uses Proprietary Interchange Protocol unknown to Third Parties (not WITSML)
- Only Two Connections: A Connection from a hardware aggregator device with full Barriers to Attack
- A second Connection to a twinned hardware device reassembling the WITSML data

Questions?

Thank you!