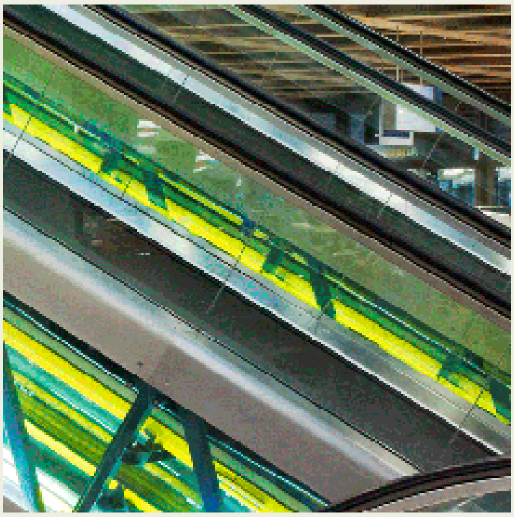
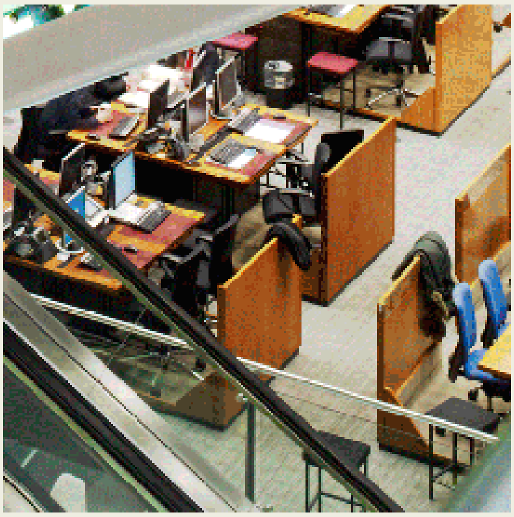


A JOINT RIG COMMITTEE REPORT

UPSTREAM OIL & GAS CYBER RISK: INSURANCE TECHNICAL REVIEW

Author: Francis Lobo, Head of Oil & Gas Engineering, Canopius

First Report, May 2018



IUA
OF LONDON
INTERNATIONAL
UNDERWRITING ASSOCIATION

INSIGHT CONSENSUS INFLUENCE

Upstream Oil and Gas Cyber Risk – Insurance Technical Review

First Report, May 2018

Acknowledgements

The Joint Rig Committee (JRC) Cyber sub-committee was formed in 2016 to further the understanding of cyber exposures within the offshore oil and gas market on behalf of the Insurance industry.

The JRC would like to give its grateful acknowledgement to DNV GL for hosting the workshop that led to the production of this report. While some of the inputs to this report are from discussions at a workshop, no statement in this report should be taken as a direction or recommendation of DNV GL.

Disclaimer

This report has been developed using information from various sources including publicly available information, initial discussions with specialists in relevant areas, pre-workshop input from participants and information from discussion at a workshop. While care has been taken in preparing this report, the Lloyd's Market Association (LMA), the International Underwriting Association (IUA), Joint Rig Committee (JRC), Canopius Managing Agents Limited (Canopius) and DNV GL do not make any representation or warranties as to its accuracy or completeness and expressly exclude to the maximum extent permitted by law all those that might otherwise be implied. The LMA, the IUA, the JRC, Canopius and DNV GL accept no responsibility or liability for any loss or damage to any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

CONTENTS

1. Executive Summary

The JRC Cyber sub-committee engaged with DNV GL to bring together various experts within a workshop, which has led to the production of this report.

Oil and Gas Vulnerabilities

- Cyber events should be considered either possible or not possible.
- The conventional Realistic Disaster Scenario (RDS) framework with event return periods may not be aligned with the risk profiles detailed in section 4.
- There may be systematic vulnerabilities in oil and gas platform design.
- Existing design parameters may be invalid or insufficient for cyber because of common cause effects.
- As assets age, if design protections are not maintained (bypassed, run for extended periods with Management of Change (MOC), etc.), cyber-related systemic risk increases.
- The weakest phases in asset life cycle are software development and commissioning.
- Software providers are relied on to test and sand-box software to ensure that it is free from malware.
- Support systems are vulnerable as they are typically sourced from lower tier vendors with fewer capabilities.
- Common Engineering network during design with access to all systems exacerbates the problem.
- Patching of Operations Technology (OT) systems is happening more frequently … increasing cyber-related systemic risk.
- Rotating equipment (compressors/generators) may have remote observers and remote maintenance and control, increasing systemic risk.
- Segregation/zoning (DMZ, CMZ, etc.) is important to reduce risk.
- Backup and restore is very important – restore capabilities are often assumed but not checked.
- There is an increasing trend to place control centres onshore with one control centre for many fields, which may introduce vulnerability.
- Field devices are being increasingly connected using wireless technology, introducing potential vulnerability into plant operating systems.
- ‘Air-gapped’ systems do not exist as all systems need to be maintained and these periods would provide a pathway for an attack.
- OT systems often have closed source software and obtaining support is difficult, and testing may be weak. Business systems have open source software: although being open source enables better testing, it does not assure absence of vulnerability.
- Ballasting operations may be vulnerable to cyber attack as modern mariners are increasingly dispensing with the traditional checks performed.
- ‘Systemic’, as defined by Lloyd’s, is ‘two or more’.

The periods of greatest vulnerability for any oil and gas installation are during the project phase when software is being developed and when patches are applied to operating systems.

Computer Vulnerabilities

Computer infrastructure in the digital era is more vulnerable than before due to the convergence of four key factors:

- The world population of computers is more homogenous than ever.
- Computing systems are more connected than ever before, enabling a fast-spreading virus to rapidly infect millions of machines.
- Computers are more programmable than ever before; even novice users can create malicious code that can control virtually every aspect of the computer system. Furthermore if a novice user does not have the resources to craft a targeted attack, these services are easily procured – anonymously (with the rise of digital currency).
- The hardware and software platforms used by big business and the home user are converging, lowering the bar to build and test malicious software.

Against this backdrop, political, ideological and criminally motivated attacks are on the rise and, due to the ubiquitous nature of the internet, some of these attacks could affect facilities and installations that are not directly being targeted. Security by obscurity is no longer considered effective because of the broader availability of information on the World Wide Web combined with an increasing trend of industry-focused cyber security research.

A developing threat is the emergence of machine learning and machine understanding: in particular, deep learning including image understanding, signal processing, and voice and text understanding. In today's world of digital communication, these capabilities could be used to increase automation or remote operation but also to deceive, and gain information, access and control over systems at the very highest levels.

Resilient Assets

Upstream oil and gas facilities (especially offshore) contain relatively low levels of inventory and their detection, automated shutdown and blowdown systems reduce individual asset and systemic exposure significantly.

The design criteria of wells, onshore or offshore, mean that in the operations phase it would not be possible for a cyber attack to result in a 'Well Out of Control' major accident scenario.

Static offshore process facilities (with the exception of HIPPS protected systems) would be adequately protected by mechanical means on almost all offshore installations worldwide and the systemic risk from a cyber event would therefore be very low.

Suggestions

A change in approach to the design of industrial facilities is required to adequately control Major Accident Hazard (MAH) risk that may arise from cyber-related scenarios.

The conceptual introduction of one or more intrinsically cyber safe devices/provisions that afford active protection against loss of containment events would be sufficient to address systemic risk. As such intrinsically cyber safe provisions would be dormant except when called upon to respond to a potentially catastrophic situation, industry would still be able to realise the enormous benefits of digitalisation while being protected against catastrophic loss and, in particular, systemic cyber-related loss.

Further work, on a facility-by-facility basis, would be required to assess the exposures and vulnerability to cyber events that might give rise to large systemic losses.

Oil and gas companies need to be engaged at the highest levels to stimulate awareness of the risks and encourage the joint participation of staff and company management to eliminate the risk to the maximum extent practicable.

2. Report Limitations and Restrictions

The JRC had previously prepared a Statement of Requirements (SOR) from which the workshop based their discussions and this SOR may be found in Appendix I. In addition to the JRC SOR, due to the timing of the workshop being limited to one day, a strict set of restrictions were placed on the scenarios that would be considered.

Only systemic risks were considered. This was deemed to be more than one insured and/or more than one asset. It was also generally considered that a systemic loss would not have any geographical limitation.

This report does not cover attacks from any of the threats that may use cyber capabilities together with other technologies, such as airborne, watercraft or submarine drones to create lethal autonomous robots capable of attacking multiple upstream facilities simultaneously.

This report documents the consensus views of the risks, based on maximum exposure scenarios above a $100 million loss threshold, for each of the upstream oil and gas facility types considered. Participants felt that, while cyber threats may be material to the frequency of losses at lower levels, it was considered that, with the magnitude and at the pace that these might occur, insurance companies/the insurance markets could adapt their practices to accommodate the evolving landscape while maintaining a viable and sustainable business.

The introduction of ‘non-physical’ concepts such as Business Interruption (BI), Loss of Production Income (LOPI), Liability and Damages (e.g. personal injury), etc. would have made the workshop process unmanageable, as the number of scenarios would have been too many to consider in a one-day workshop. With BI, LOPI, etc., even small Physical Damage (PD) scenarios can result in disproportionately large losses. It is important to note here that, while insurers may, in certain circumstances, consider endorsing a policy with a write back to the Cyber Attack Exclusion Clause CL380 to provide cover for BI/LOPI, it was decided that the $100 million loss threshold would relate to PD and third party liability (for environmental PD) only.

The workshop assumed that in ‘cyber space’ elimination of ‘the threat’ is virtually impossible as the sources of the threats (especially new threats) are unknown, with current remedies at best eliminating the risk arising from known threats. Due to the importance of defence and detection in depth to all loss levels, a section of this report (Appendix IV - Cyber Defences) is devoted to the practical measures that may be employed in this area. Development of any framework relating to the provision of insurance cover for cyber-related risk would need to place significant emphasis on these as well as other aspects related to Major Accident Hazard (MAH) risk highlighted in this report.

3. Workshop Structure and Considerations

The workshop sought to understand the extent to which the various types of upstream facility might be inherently vulnerable to attack (including considerations of facility design) for different cyber attack types for major loss/catastrophic loss events. The extent to which systemic risk existed above the $100 million PD loss threshold for each MAH scenario was also debated and the author's conclusions are documented in this report.

The methodology adopted for the workshop was to convene participants covering the following relevant disciplines/stakeholder groups to assist the author in the understanding of risks and threat processes:

- Process Engineers
- Cyber Security Experts
- Control System Experts
- FPSO Design/Hull Strength Leads
- Dynamic Positioning (DP) Experts
- Lloyd's Performance Management Representative
- Lloyd's Market Association (LMA) Representative
- Insurance Underwriters
- Insurance Engineers

Upstream facilities were grouped into constituent parts as follows:

- Wells (Offshore and Onshore)
- Well-site Installations (including Subsea)
- In-field Lines, Risers and Pipeline Systems
- Offshore Platforms (Fixed and Floating)
- DP Vessels
- Onshore Facilities and Storage (including Oil Terminals, Tank Farms and Underground Gas Storage)

The worst MAH scenario possible for each of these constituent parts was assessed, with onshore and offshore installations considered separately, as appropriate. On occasion, for floating facilities, for example, the primary major accident loss scenario, Fire and Explosion (F&E), would have been captured during discussions relating to fixed platforms but an alternative major accident loss scenario, such as sinking, was also potentially vulnerable to cyber attack and therefore captured during discussions.

The slate of MAH scenarios considered was as follows:

<u>Wells:</u>

- Onshore – F&E – Open tree valves to external environment
- Offshore – F&E – Open tree valves to external environment
- Drilling – Blowout – Tamper with rig systems; Defeat Blowout Preventer (BOP) protections

• Subsea	– Loss of Containment – Open valves to external environment

Offshore Platforms:

• Fixed	– F&E – Tamper with process systems/Defeat protections (F&G, HIPPS, etc.)
• Floating	– F&E and Water Ingress (Sinking) – Tamper with ballasting/ sea chest valves

In-field Lines, Risers and Pipeline Systems:

• Onshore (Largest Lines)	– Overpressure line. Defeat overpressure protections
• Submarine (Largest Lines)	– Defeat iHIPPS protections. Collapse line

DP Units:

• Rigs	– Blowout – DP tamper moves rig off well. BOP protections defeated
• Other	– DP tamper causes drive-off and collision with adjacent facility

Onshore Processing, Storage, etc.:

• Wells/CPF	– F&E – Tamper with process systems. Defeat protections
• Terminals	– F&E – Tamper with tank filling systems. Defeat protections
• FPSO/FLNG/FSRU	– F&E and Sinking – Ballasting or overpressure hull below waterline
• Underground Gas Storage	– F&E - Tamper with process systems/facilities. Overpressure underground reservoir. Defeat protections

4. Workshop Results

The workshop addressed several discussion areas as follows:

- There may be systematic vulnerabilities in oil and gas platform design.
- Existing design parameters may be invalid or insufficient for cyber because of common cause effects. Namely, when designers consider that, for example, if a certain valve fails, then another valve in series will stop the event from developing; they typically do not consider the possibility that both valves may fail together because of a common cause event (e.g. cyber-initiated).
- As assets age, if design protections are not maintained (bypassed, run for extended periods with Management of Change (MOC), etc.), cyber-related systemic risk increases.
- Weakest phases in asset life cycle are software development and commissioning.
- Software providers are relied on to test and sand-box software to ensure it is free from malware.

- Support systems may be vulnerable as they are typically sourced from lower tier vendors with fewer capabilities.
- A common engineering network during design with access to all systems exacerbates the problem. This is because lower tier vendors with perhaps less sophisticated cyber defences may access the entire network and permit malware to infect the system or allow malevolent persons access compromising the system integrity.
- Operations Technology (OT) systems are becoming more aligned with traditional Information Technology (IT) systems – which require more frequent updating that, while recommended security practice, does increase the risk of malware being introduced via an update.
- Rotating equipment (compressors/generators) may have remote observers and remote maintenance and control (remote services), increasing systemic risk. In general, dynamic systems (compressors, thrusters, etc.) were considered to be more vulnerable to the cyber threat than static systems (separators, heat exchangers, etc.). It was observed that significant systemic risk might be introduced due to the vulnerability of remote services to these types of equipment, which, while individually might not breach the $100 million threshold, could represent significant PD exposure to the insurance markets as supply/demand and manufacturing facility limitations push the replacement cost of systemically affected equipment far beyond expectations.
- Segregation/zoning (DMZ, CMZ, etc.) is important to reduce risk.
- Backup and restore is very important – restore capabilities are often assumed but not checked.
- An increasing trend to place control centres onshore with one control centre for many fields introduces vulnerability. IT hubs onshore are in buildings and if the building management system is attacked, this could take out air conditioning to multiple IT hubs and cause significant production outages. This is an example of attack on a seemingly lower tier system (less well defended) having a significant production impact. This scenario is not likely to involve explosions, etc., as production facilities are equipped with 'fail-safe' equipment.
- Field devices are being increasingly connected using wireless technology, introducing potential vulnerability into plant operating systems.
- 'Air-gapped' systems do not, in practice, exist as all systems need to be maintained and these periods would provide a pathway for an attack.
- OT systems often have closed source software and obtaining support is difficult, and testing may be weak. Business systems have open source software: although being open source enables better testing, it does not assure absence of vulnerability.
- Ballasting operations are vulnerable to cyber attack as modern mariners are increasingly dispensing with the traditional checks performed.
- 'Systemic', as defined by Lloyd's, is 'two or more'.

It is important to note that the workshop was of the consensus that cyber events should be considered either possible or not possible (plausible or not plausible). Participants were led to the conclusion that the conventional RDS framework (with event return periods, etc.) may not be aligned with the risk profiles that were discussed. This is because the threat actors are unknown, especially as an attack might manifest as a collateral effect from the actions of malevolent persons seeking a different target. Additionally, the full range of potential delivery vectors is unknown.

As insurance markets routinely provide insurance cover for LOPI/BI, if these coverages are being provided to include cyber perils, further work on a facility-by-facility basis would be required to assess the exposures and vulnerability to cyber events that might give rise to large systemic losses.

In particular, there was disagreement on whether ‘fixed offshore platforms’ had at least one ‘cyber safe’ risk reduction barrier, and it is likely that this category would need to be further subdivided as, in the author’s opinion, more than 95% of offshore platforms insured worldwide are designed with mechanical relief valves or bursting discs connected to relief lines with unobstructed pathways to the flare or vent stack. There was concern expressed about the move towards further automation which, in seeking to minimise labour costs and exposure to hostile environments, could introduce cyber vulnerabilities to sensitive systems. Similar debate concerned whether catastrophic loss of floating facilities could be caused by ballasting systems.

A major differentiator identified at the workshop was that upstream oil and gas facilities (especially offshore) contained relatively low levels of inventory (compared to onshore and downstream facilities) and were heavily instrumented with detection, automated shutdown and blowdown systems, which serve to reduce individual asset and systemic exposure significantly.

Offshore facilities are designed to not only exploit oil and gas but also provide a safe environment for people living on the facility while considering they do not have an easy means of escape. Platforms are therefore designed to shut-in the almost inexhaustible inventories in the reservoir and pipelines/risers and blowdown the hydrocarbon inventories (via flare or vent) in the facilities within 15 minutes of event detection.

The heat map follows below, with red indicating that systemic risk resulting from cyber was judged to be possible and green indicating it was judged to be not possible. Further work may well demonstrate that some of the categories/scenarios showing as red on the heat map become green in the context of the provision of insurance cover.

The threat levels in the table below are categorised as follows:

- Level 1 - Non-Targeted Specific – Installation/company specific (Operator error, IACS software errors, etc.).

- Level 2 - Non-Targeted Generic – Viruses, Bugs, Faulty Software (could be innocent or malicious or collateral effects from Level 3 or Level 4 attacks aimed at a different target).

- Level 3 - Targeted virtual component only – Hacktivists, Criminal (limited technical capabilities), Recreational, etc.

- Level 4 - Targeted with virtual and physical components including an ability to deploy (or influence actions) physically at site - excluding particular individuals, operators, drillers, etc. – State sponsored, Organised crime, etc.

Upstream Cyber Heat Map

Analysis assumes protective systems are well maintained

Facility Types	MAH Scenario	Threat Level 1	Threat Level 2	Threat Level 3	Threat Level 4
Wells					
Onshore	F&E: Open Tree Valves to external environment	🟩	🟩	🟩	🟩
Offshore	F&E: Open Tree Valves to external environment	🟩	🟩	🟩	🟩
Drilling Systems	Blowout: Tamper with rig systems. Defeat BOP protections	🟩	🟩	🟩	🟩
Subsea Installations (inc. subsea wells)	LOC: Open valves to external environment	🟩	🟩	🟩	🟩
Offshore Platforms					
Fixed	F&E: Tamper with process systems/facilities. Defeat protections (F&G, HIPPS, etc.)	🟩	🟥	🟥	🟥
Floating	W: Tamper with ballasting/Sea Chest Valves. F&E same as Fixed above	🟩	🟥	🟥	🟥
In-Field Lines, Risers and Pipeline Systems					
Onshore (Largest Lines)	F&E: Overpressurise line. Defeat overpressure protections	🟩	🟥	🟥	🟥
Submarine (Largest Lines)	W: Defeat iHIPPS protections. Collapse line	🟩	🟥	🟥	🟥
DP Units					
Rigs	Blowout: DP tamper moves rig off well. BOP protections defeated	🟩	🟩	🟩	🟩
Other	C: DP Tamper causes collision with adjacent facility	🟩	🟥	🟥	🟥
Onshore Processing , Storage					
Onshore Processing (Well site and CPF)	F&E: Tamper with process systems/facilities. Defeat protections	🟩	🟥	🟥	🟥
Oil Terminals	F&E: Tamper with tank filling systems. Protections defeated	🟩	🟥	🟥	🟥
FPSO/FLNG/FSRU Storage	Catastrophic Loss: Ballasting or over pressuring hull below waterline	🟩	🟥	🟥	🟥
Underground Gas Storage	F&E: Tamper with process systems/facilities. Defeat protections	🟩	🟥	🟥	🟥

Legend:		
	MAH	Major Accident Hazard
	F&E	Fire & Explosion
	W	Water Ingress
	C	Collision or Allision
	LOC	Loss of Containment

Another key finding of the workshop was that current design parameters may be invalid or insufficient for the cyber threat because of common cause failure. This leads to a conclusion that a change in philosophic approach to the design of industrial facilities is required to adequately control MAH risk that may arise from cyber-related scenarios.

However, it is worth noting that, to minimise the risk of cyber-related losses, the cyber strategy of an operating company would be of paramount importance, defending and detecting in depth. Defence in depth is highly effective in military situations because the strategy delays the advance of an attacker but critically permits time to launch a counter-attack to eliminate the threat.

As many losses, such as the Olympic Pipeline loss that was caused by a wrongly configured Pressure Relief Valve (PRV), result from the compromising of other barriers, the facility assessment should incorporate a view on the likely efficacy of the 'cyber safe' barriers as they exist at the facility. Insurers would then be able to build up a picture of the systemic risk associated with their portfolio of assets being insured.

In any event, it is recommended that data is captured relating to OT systems/dynamic equipment (compressors, generators, etc.)/number of independent systems controlling risk reduction and consequence reduction barriers, etc. at each facility, so insurers may gain an understanding of the diversity of their portfolio and assess their robustness to systemic cyber risk, noting, of course, the difficulties in quantifying cyber risks identified elsewhere in this document.

Also, while this report primarily addresses technical aspects, it is important to note that cyber assurance measures cover both technical measures (technology) and system measures (man and organisation). It was felt that the upstream oil and gas industry needs to undergo similar processes with cyber risk to those that occurred with Health and Safety risks over the past 30 years in the wake of the Piper Alpha disaster. With Health and Safety risk, oil and gas companies engaged at the highest levels to stimulate awareness of the risks and encourage the joint participation of staff and company management to eliminate the risk to the maximum extent practicable. The result was transformative success, changing the risk culture and attitudes across the whole industry.

Finally, in respect of the insurance-specific question of whether forensic analysis could determine that an event resulted from a cyber attack, the conclusion was uncertain. Determination of the perpetrators would depend on the event and the IT and OT provisions that were in place at the time of the attack. It was noted that the detailed computer logs that would be required for forensic analysis were often maintained at site (offshore), with enterprise management systems not capturing information to the level of granularity that would be required. Therefore, if the site facility (in particular records at site) were destroyed in an event, it may not be possible to forensically determine whether or not the root event was cyber-initiated.

It is hoped that the contents of this report may assist with the development of a framework to classify and assess the cyber risk profiles of individual upstream installations. Such profiles could be used to facilitate the considered provision of insurance cover for cyber-related events for upstream oil and gas facilities.

5. Background

A workshop was hosted at the DNV GL offices in London during December 2017 where subject matter experts were available to identify threats and likely scenarios for insurance representatives to consider. The aim of the workshop was to discuss systemic risk that may arise out of the cyber consideration and derive RDSs for the systemic cyber threat in the context of upstream oil and gas facilities.

The underwriting of upstream oil and gas facilities is structured to manage exposures associated with catastrophic incidents which have an extremely low occurrence frequency (excepting certain natural hazard exposures). Insurance companies are positioned to manage a single catastrophic loss (or even several, depending on the loss quantum, the size of the insurer and the insurer's participation on the risks) whether they arise from an accident, operational incident or cyber attack. However, the emergence of cyber as a potential threat source raises a fundamental question for insurance companies and their reinsurers: namely, how much systemic risk is introduced due to the cyber threat component and is the systemic exposure manageable?

While the digital age brings with it enormous benefits ranging from cost-efficiencies, revolutionary business and servicing models, advanced knowledge paradigms and associated opportunities, it also brings with it threats that have the potential to be debilitating to a company, an organisation and even nation states.

Oil and gas companies are lucrative targets for cyber attackers motivated to perform industrial espionage, steal intellectual property, cause PD or engage in indiscriminate criminal activity involving blackmail and ransom demands. As energy security is of fundamental importance in the modern world, oil and gas companies can also inadvertently be drawn into political and global theatres of engagement.

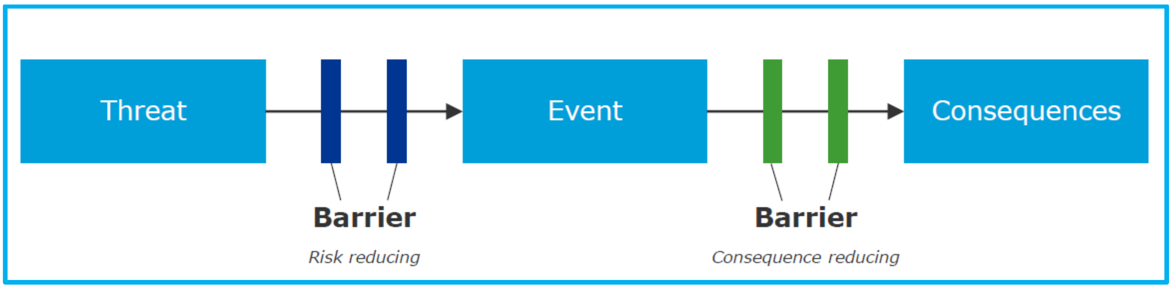
Many of the threats arise in the IT domain, which is predominantly virtual, but threats to physical assets, personnel safety and the environment have emerged as OT environments converge with IT environments. Critical infrastructure is increasingly fusing these two different technologies together using open IT protocols, OT with Supervisory Control and Data Acquisition (SCADA) and enterprise IT systems. There is also an increase in connections between OT environments, the internet and cloud-based systems. The integration of Distributed Control Systems (DCSs) with Safety Instrumented Systems (SIS) is also on the increase (e.g. Yokogawa Prosafe RS system).

It should be noted that, while the threat landscape in the virtual world is continuously changing, so are the institutional responses (cyber strategies and cyber defences employed). In addition, the physical facilities and their 'hardwired' defence systems also continue to change to take advantage of evolving technologies with the aim of increasing operational efficiencies or for increased safety and reliability. Such technologies include remote operations, increased use of wireless systems and of encryption systems. Key to the increased use of encryption systems is the reduction of the physical footprint of the equipment required for the higher computing speeds necessary for OT applications.

Malware can spread rapidly across the globe. The Sapphire worm (aka Slammer worm) in 2003 doubled in size every 8.5 seconds. It infected more than 90% of vulnerable hosts within 10 minutes. Sapphire did not carry a malicious payload but it caused considerable harm by overloading networks and taking database servers out of operation, resulting in cancelled flights, interference with elections and Automated Teller Machine (ATM) failures. It was the first malware to demonstrate that fast worms in the wild were not just a theoretical possibility but a real threat.

Wannacry (May 2017), the biggest ransomware attack in history, spread across the globe in just a few hours, affecting the National Health Service - UK, Iberdrola Natural Gas - Spain, Interior Ministry - Russia, Megafon – Russia, Library – Oman, Railroad System - Russia, Sherbank - Russia, Shaheen Airlines – India, Secondary Schools and Universities - China, Yanshui County Public Security Bureau – China, Renault – France and the University of Milano – Italy, among others.

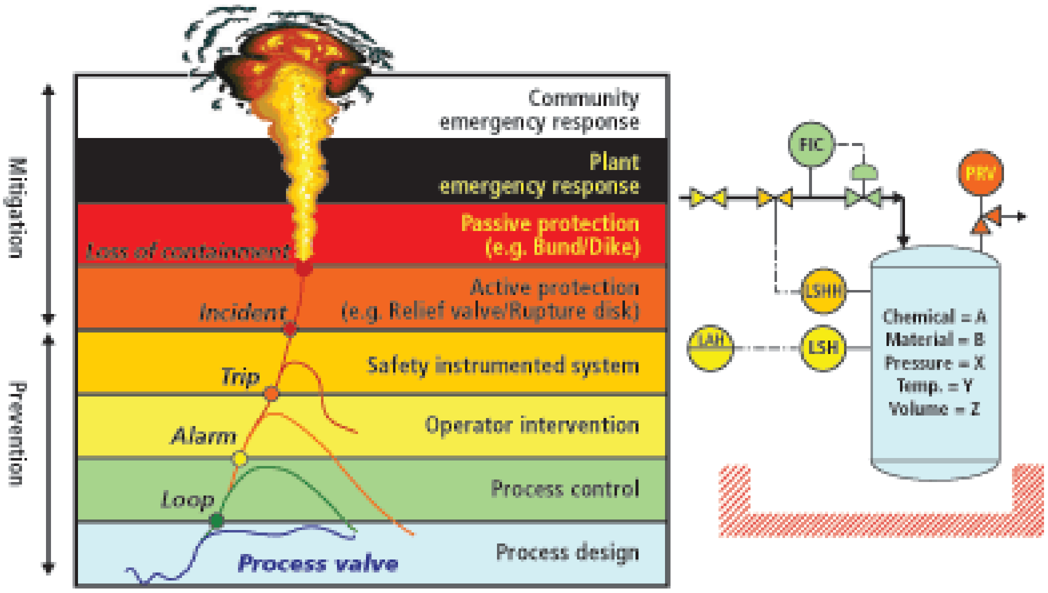
The following graphic illustrates the design methodology currently in use when considering accident scenarios.



From DNV GL

Designers of industrial facilities test their designs against various threats, for example high pressure, and consider what 'barriers' there may be in place to prohibit an event from manifesting. In the case of the high pressure example, designers may consider that there are 'risk reducing' barriers (left-hand side in the figure above) such as upstream chokes regulating the pressure, valves shutting in or valves opening relieving the high pressure. 'Consequence reducing' (right-hand side in the figure above) barriers might be Fire and Gas (F&G) detection systems, deluge activation systems or shutdown and blowdown systems.

Another way of viewing the design process for facilities is using the concept of Layers of Protection. The figure below illustrates the concept:



Source: ISA, InTech Magazine, 2009

Currently, there is no requirement in any of the design standards that one or more of the ‘risk reducing’ barriers or active protection layers that may prevent an incident from resulting in a loss of containment must be inherently safe from cyber events. For MAH scenarios, if a design requirement were to be that one or more of the ‘risk reducing’ barriers or layers of protection must be inherently cyber safe (by physical limitations, mechanical devices or other intrinsically cyber safe devices) then cyber-related systemic risk might be considered to be adequately addressed.

Industrial automation and control systems (IACS) such as SCADA, DCS, Programmable Logic Controllers (PLCs), Object linking and embedding for Process Control (OPC) servers, Field Devices and other critical components are generically referred to as OT or IACS/Industrial Control Systems (ICS). The terminology that will be used in this document is IACS and OT, used interchangeably.

Historically SCADA and DCS were different - one kind of software could not control the other kind of process. Nowadays, general purpose control system software has all the features of both SCADA systems and DCSs so the difference between the two terms is more of usage than technology.

The role of IACS/OT is the acquisition of data coming from processes (pressures, temperatures, valve positions, chemical compositions, tank levels, etc.) and the direct control of electrical, mechanical, hydraulic or pneumatic actuations based on acquired data as processed by system control models.

In the past (and still at locations worldwide) OT networks were air-gapped from business networks (office network) and the internet. They were operated using proprietary hardware, software and communications protocols. However, in recent years, demand for business insight, requirements for remote network access and the spreading of hardware and traditional IT software (e.g. Ethernet, TCP/IP networking, Windows-based platforms) has caused many oil and gas companies to integrate control systems and their enterprise IT systems, with some even providing access to the OT network from the cloud. Obsolescence and the inability to procure vendor support for legacy systems is often the reason for change. The integration of control systems and business systems increases the exposure of business critical systems and devices to external disruptors such as Trojans, worms, viruses and hackers.

It should be noted, too, that ‘air-gapped’ systems may also be connected systems when updates are being performed or when maintenance is being carried out. Engineers may bring firmware updates on, for example, memory sticks, which have the effect of bridging the airgap and allow the insertion of malware onto a system that is considered to be safe from malware because of its air-gapped nature.

Systems Applications and Products (SAP) (ABAP, J2EE Mobile, HANA, and Business Objects) and Oracle (EBS, Peoplesoft, JDE, Siebel) applications are very common in upstream oil and gas companies. SAP is used to bring together many technical disciplines and business functions that are loosely connected. SAP aims to leverage across a common platform for operations and maintenance, enabling data to be gathered, analysed, decided upon and executed across many elements driving performance across the different life cycle stages.

In integrated digital oilfield operations, SAP is used to integrate production, maintenance and engineering operations, closing the gap between decision-making and in-field execution. In these applications (SAP EAM/PM and SAP UOM), there is potential for PD to production and engineering devices.

SAP has over 246,000 customers worldwide, including 85% of Fortune 2000 Oil and Gas. Oracle applications are used by 100% of Fortune 100 companies.

SAP interfaces with SCADA and DCS systems that are provided by specialist automation and control system providers. The leading ten such companies in oil and gas are:

- ABB Ltd. (Switzerland)
- Honeywell International (US)
- Siemens AG (Germany)
- Schneider Electric (France)
- Mitsubishi Electric Corporation (Japan)
- Yokogawa (Japan)
- Rockwell Automation (US)
- Emerson Electric Company US)
- Cameron International Corporation (US)
- Texas Instruments (US)

ABB ranks first, by DCS market share, in the world's upstream oil and gas industry and has installed over 10,000 sets of its flagship 800xA systems alone in more than 100 countries worldwide.

Another company worthy of specific mention is Kongsberg Marine (Norway) due to its DP systems, which account for approximately 80% of those used in upstream oil and gas high-end activities.

It was noted that the larger system vendor companies were more difficult to affect with a cyber attack (or hack) as greater institutional resources are employed and the levels of cyber security are high. Smaller vendors could be the weaker links due to the variety of systems in use, with these vendors often not having the resources or skills to secure systems to the highest standard.

However, the Apple MacOS password vulnerability (2017) that permitted individuals to log into Macs as administrators with super-user privileges without passwords illustrates that threats in the 'cyber world' can develop from the unlikeliest of sources and the more ubiquitous the company, the higher the systemic risk.

It is important to note that the industrial systems used in the world's upstream oil and gas industry are also used by other industries. The Stuxnet worm targeted centrifuges at nuclear facilities but it also seriously affected oil refineries, gas pipelines and power plants as it was designed to reprogram the control systems managing the industrial environment.

ICS vulnerabilities can be introduced from ancillary functions such as the data historian. A data historian typically resides in a less secure zone (i.e. the business network) but collects and stores information centrally. Proprietary data collectors are deployed close to the production equipment and associated ICS components (allowing high frequency data collection) and replicate to a central 'shadow' server that relies more on standard technologies like the Microsoft Sequence Query Logic (SQL) server and Oracle. A data historian could be used as a vector into more secure zones. OSIsoft holds a dominant position in the data historian market (65% in 2015) and integrates with many IT and OT systems.

A key cyber vulnerability of oil and gas facilities illustrates the issue of how difficult it is to ensure that these critical systems are defended comprehensively. The periods of greatest vulnerability for any oil and gas installation are during the project phase when software is being developed (often quite far down a supply chain), the commissioning phase (when the intensity of activity means that traditional security protocols may not be enforced) and also when patches are applied to operating systems, for example during upgrades.

These are 'open door' periods when time-triggered code could be embedded directly into instrumentation and systems. This would defeat system perimeter defences (firewalls, etc.) and intrusion detection systems (IDS). The systemic effects of such an attack if it were perpetrated on a major supplier could be of global significance.

However, while this is a plausible route to execute an attack with significant systemic consequences, the view at the workshop was that any programmable automated and/or instrumented function was capable of being attacked regardless of system architecture, process zones, safety zones or the number of 'independent systems' involved. These arrangements were considered to be deterrents/obstacles but could not be relied upon to afford ultimate protection against cyber attacks, some of which could have systemic consequences.

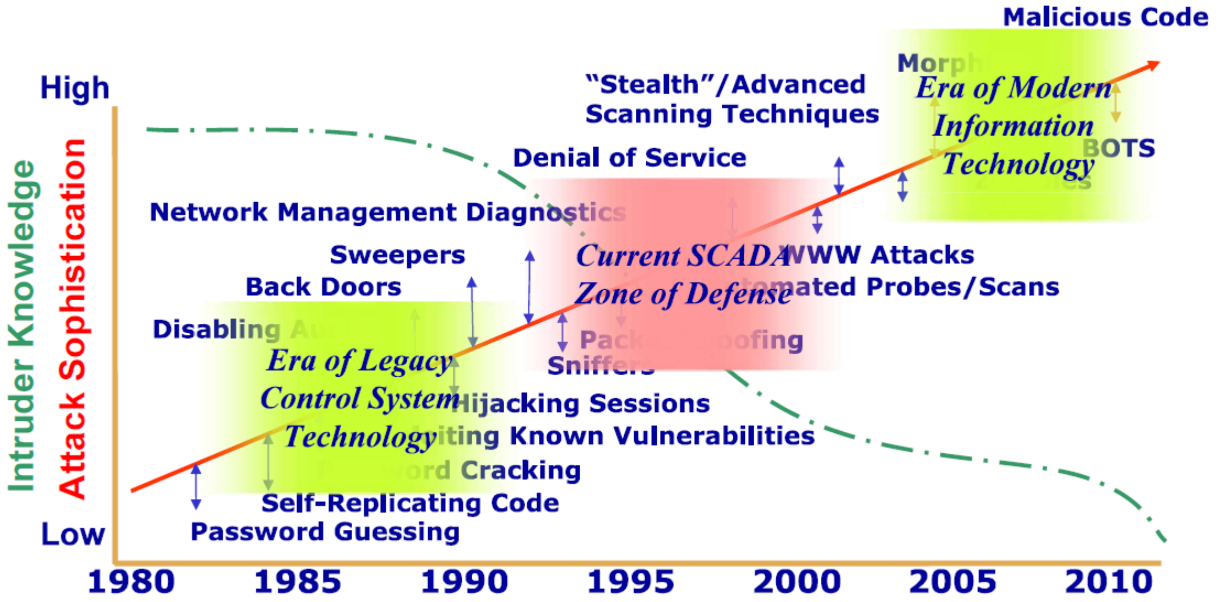
A Deloitte report published on 26th June 2017 found that three-quarters of US oil and gas companies experienced at least one cyber incident in 2016 while, at the same time, noting that fewer than half of these companies used any monitoring tools on their upstream operations networks and only 14% had fully operational security monitoring centres.

IT strategies also have a part to play, as employee vulnerability through lack of threat awareness, falling victim to sophisticated social engineering ploys, coercion/blackmail or simply the selling of company security information on the dark web driven by the profit motive can increase network vulnerability. The global outsourcing of IT functions to developing countries in the pursuit of cost savings or operational efficiencies can also increase risk if vetting protocols, access controls, loss of management control and the ultimate enforcing of accountability in the relevant jurisdiction proves to be inadequate.

It is almost a certainty that future threats will use machine learning and understanding to try to outsmart cyber defences. It is speculated that the future of cyber security will be warfare of machine learning/understanding techniques with the most capable machine learning/understanding techniques winning the day.

The graphic (from 2002) on the following page from the U.S. Department of Homeland Security charts the evolution of cyber threat trends.

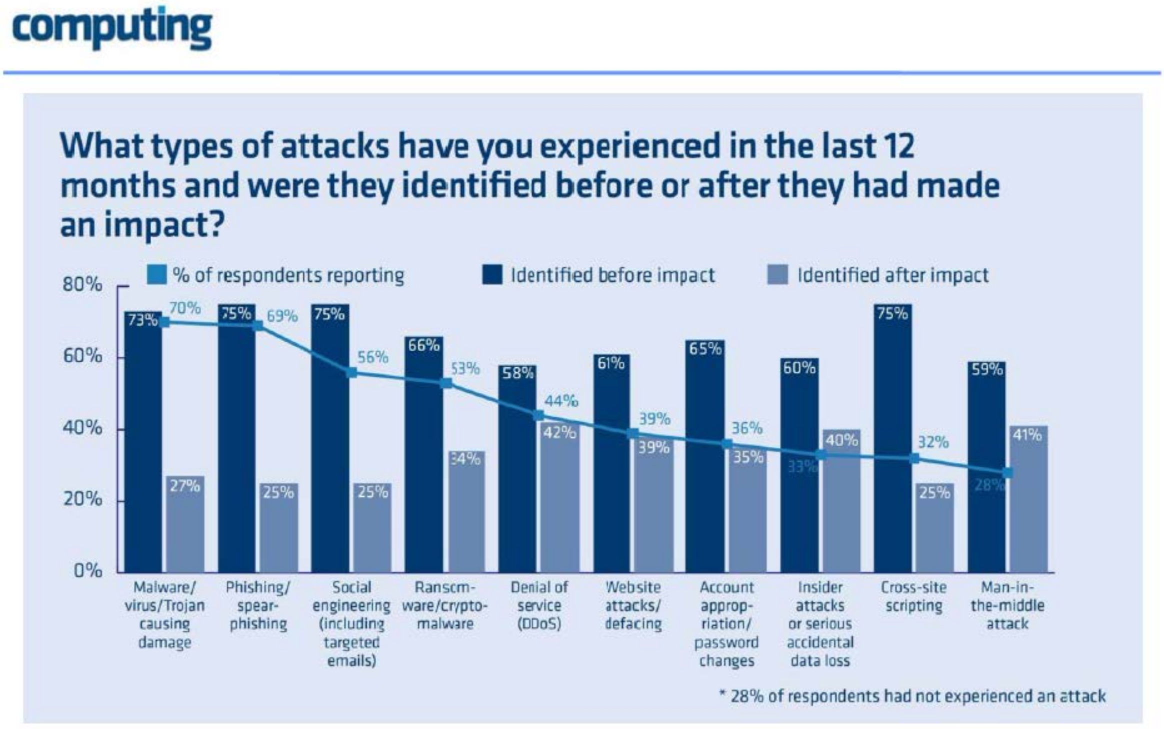
Threats become more complex as attackers proliferate



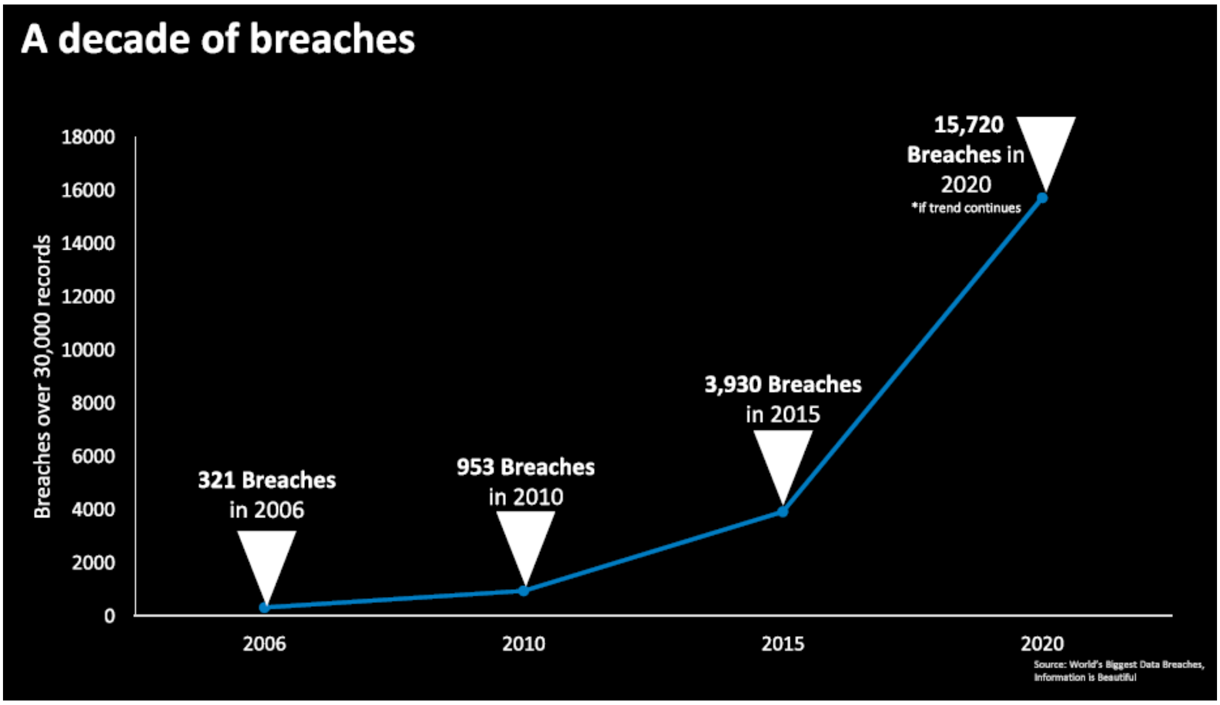
Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

Homeland Security

A survey of senior executives in 2017 across a range of companies provided *Computing* magazine with the statistics presented in the graphic below:



Interesting take-aways from this are that 1) 72% of companies surveyed reported being attacked and 2) the success rate of an attack was in excess of 25% (attacks identified after impact) for all categories of attack, with some types of attack having over 40% success rate. Also, data breaches are on an increasing trend as the graphic below illustrates:



Cyber capability is developing at a rapid pace, both with regard to nation states and criminal organisations, and is demonstrated by the figure above.

With the ever-increasing attack surface available to potential perpetrators, there is a trend among company security officers to accept that it is impossible to defend the perimeters of their IT systems and the focus is shifting from defence to detection and rapid response.

This arguably may be acceptable in an IT domain, although even data loss, etc. could be very damaging and potentially devastating. However, in OT domains, intrusions could (and have) led to catastrophic outcomes.

6. Cyber Events

The recorded events below were collated from publicly available information and, as they have not been corroborated at source, could be subject to bias. It is therefore important to note that a basic premise of this report is that it is assumed cyber threats are real and ever-present in the modern cyber-enabled world.

While the below historic data below (and more that could be gathered) might be able to be used to derive return period estimates for cyber RDSs, it is felt that these would be largely fictitious if an attempt was made to project on this basis into the future. As cyber is rapidly evolving, in terms of technologies, threat actors and threat vectors, it is highly likely that the future landscape will bear no resemblance to the current and past landscapes.

Upstream Events

1999 A Trojan was delivered to a Gazprom company insider who opened it deliberately. The entire control system of the Russian gas supplier was under direct control of the attackers for a number of hours.

2008 An IT consultant (Mr Mario Azar) who felt aggrieved after not having been offered a permanent position in the Networks Operations Centre (NOC) for Pacific Energy Resources in Long Beach California, still with access rights, disabled the leak detection system on three offshore platforms. A single NOC can control up to 50 oil platforms, providing a single point of entry to a huge number of targets.

2010 A rig en route from South Korea to Brazil was so riddled with computer malware that it took 19 days to make it seaworthy again. While this is not an attack, it is a demonstration of the potential for loss arising out of a cyber event.

2011 A Night Dragon attack disabled proxy settings and, for years, used remote administrative tools to steal sensitive information, including operational oil and gas field production systems (including ICS) and financial documents related to field exploration and bidding data on oil and gas assets of many oil and gas companies (including supermajors).

2012 Shamoon malware was used to inflict a cyber attack on Saudi Aramco, damaging at least 30,000 computers. Shamoon spread promiscuously and wiped systems clean while corrupting the master boot record leaving the computer inoperable. The attack aimed to disrupt oil and gas production in Saudi Arabia and prevent resource flow to international markets. Luckily the destruction did not spread to industrial network areas and therefore did not directly impact oil production, refining, transportation or safety operations. It is believed that this was Iranian malware developed in retaliation against the West for Stuxnet's sabotage of Iranian nuclear ambitions at the time.

2012 Televent, a supplier of remote administration and monitoring tools to the energy sector, became a victim of a sophisticated advanced persistent threat that breached its internal firewall and security systems. Televent stated that every Fortune 100 energy company relied on their systems and information to manage their business, managing over 60% of the total hydrocarbon movements in North American and Latin American pipelines.

2014 Dozens of oil companies (including Statoil) in Norway were targeted with cyber attacks. The attackers have not been identified and motives remain unclear.

2017 A company's SIS (in the Middle East) entered a fail-safe state, shutting down all industrial processes for no apparent reason. The root cause was identified to be the presence of malware known as Triton (aka Trisis), which was designed to target equipment manufactured by Schneider Electric, a company which supplies equipment used in oil and gas facilities and also sometimes nuclear energy facilities and manufacturing plants. This attack marks the first reported breach of a safety system at an industrial plant by hackers.

Triton appears to be designed to tamper with or even disable SIS as well as DCS (made by a separate company) used by operators to monitor and manage industrial processes. In this event the attacker(s) had control of the safety systems as well as the DCS and could have used this control to cause explosions, oil spills, etc. with devastating results.

Other Events

1999 Erroneous changes to a live historical database caused critical slowdown in system responsiveness (sensor scan rate changed from 3 second poll to over 6 minutes) in a 16' Olympic Pipeline Company gasoline pipeline in Bellingham, Washington, USA. This, combined with a PRV that was not configured properly and failed to open, caused a pressure surge, pipeline rupture and explosion when an automatic valve shut. Three people died and eight people were injured. Property damage was estimated at $58.5 million and the legal settlement was $112 million.

2003 A bug in the computer code of a power management system caused a blackout that affected homes across eight states in the US and Canada.

2003 Ohio's Davis-Besse nuclear power plant network was penetrated by the Slammer worm, disabling a safety monitoring system for over 5 hours before the compromise was noticed.

2005 Critical alarms and control instrumentation provided false indications that failed to alert operators of the high level of flammable hydrocarbons in the raffinate splitter tower at British Petroleum's (BP) Texas City refinery. This resulted in an explosion that killed 15 people, injured 180, shut the refinery down for a year and cost BP $1 billion in various kinds of damages. *This was not attributed to cyber attack nor is the refinery an upstream facility. It has been included in this list to illustrate the potential scale of an event at onshore upstream process and storage facilities as the false indications could equally have been a result of a cyber attack.*

2008 Alarms and communications were interfered with on the Baku-Tiblisi-Ceyhan pipeline in Turkey, over-pressuring the line and causing an explosion and the spilling of more than 30,000 barrels of crude oil.

2009 An explosion in Bayamon, Puerto Rico, was attributed by investigators to a 'glitch' in the facility's computerised monitoring system. A storage tank being filled with gasoline from a ship docked in the San Juan harbour overflowed continuously due to the malfunctioning of the tank's meter until the vapour cloud met an ignition source. The fire blazed for 3 days.

2010 Stuxnet used the Microsoft® Windows® operating systems and networks, sought out Siemens Step7 software and caused the fast-spinning centrifuges at Iranian nuclear enrichment facilities to over-speed, tearing themselves apart. The Stuxnet worm began to infect ICSs as early as 2007. It infected over 200,000 computers and caused 1,000 machines to physically degrade.

Stuxnet is extremely sophisticated in that it is programmed to operate differently depending on its environment (mutate). Stuxnet spreads, attempts to inject PLC code, communicates, self-updates, lies dormant or awakens depending on changes to its environment.

While Stuxnet was thought to have been created by western governmental agencies to target centrifuges at nuclear facilities in Iran, it seriously affected energy companies as well (oil refineries, gas pipelines and power plants) and has therefore been included in this list.

A worm called Duqu is thought to be based on Stuxnet. However, unlike Stuxnet, Duqu does not contain any code related to ICS and does not self-replicate. Duqu is, however, highly targeted towards a limited number of organisations including those involved in the manufacture of ICS. Duqu appears to be designed to gather intelligence for a future attack.

While, due to the heightened awareness of the Stuxnet code, it is very unlikely that any of the code will be reused for an attack on a different type of network/hardware, the sophisticated philosophies developed for Stuxnet could be used in a new piece of malware.

2016 The Indestroyer (aka Crash Override) malware shut down the power grid in Kiev, Ukraine (widely believed to be the work of a team of Russian government hackers known as Sandworm that has waged a cyber war on Ukraine since 2014). Indestroyer, with minor adjustments, is capable of targeting other types of critical infrastructure including pipeline control systems.

Indestroyer was not designed to look out for protocol vulnerabilities: it was designed to teach the malware to ‘speak’ those protocols and gain direct control of switches and circuit breakers. The problem is that those protocols were programmed decades ago when industrial systems were designed to be isolated from the outside world.

Indestroyer includes features that are designed to enable it to remain under the radar, ensuring the malware’s persistence and to wipe all traces of itself after it has done its job. Due to this ability to persist in a system and provide valuable information, attackers could adapt the malware to any environment, making it highly customisable and extremely dangerous.

APPENDIX I.

JRC Statement of Requirements

Upstream Oil & Gas
Cyber Risk – Technical Review
JRC Statement of Requirements (SOR)

Objective:

Based on a series of workshops involving cyber security experts, white hat hackers, operations technology practitioners and upstream insurance underwriters, the author has developed a report for the Joint Rig Committee (JRC) articulating the risks and exposures primarily in relation to the provision of cover on the basis of the Cyber Attack Buy Back Endorsement (CABBE) form but also assessing the likely systemic risk associated with each risk category.

Parameters for the workshops and report:

- Upstream facility types to be addressed:
  - Wells (Offshore and Onshore)
  - Offshore Platforms (Process)
  - Subsea Installations
  - Pipeline Systems (Submarine and Onshore)
  - Drilling Systems
  - Dynamically Positioned Units (Rigs and Other)
  - Onshore Oil Processing and Gas Processing Facilities
  - Oil Storage Terminals
  - Underground Gas Storage

- Covered perils:
  - Fire
  - Explosion
  - Water Ingress
  - Collision or Allision
  - Well Out of Control

- Types of cyber threat:
  - Malicious (Targeted and Non-Targeted)
  - Non-Malicious (Specific and General)

- Post event:
  - Ability in each case to prove forensically that the event was initiated by a cyber threat

The workshop should use a Computer/Control Hazards and Operability Study (CHAZOP)-type methodology (i.e. structured and scenario-based) to qualitatively assess the likely risk and related exposures for the largest exposure scenario(s) for each type of facility. The reviewers should assess significant system architecture types with due regard to system vintage, consider delivery vectors (entirely virtual or involving real-world interventions) and explore if, with appropriate mitigations, the cyber risk profile for the relevant scenario could be materially reduced.

APPENDIX II.

Workshop Participants

Insurance Market Workshop Participants
Hosted by DNV GL

DNV GL Attendees

Marcus Flint – Workshop Facilitator
Senior Principal Consultant, Due Diligence

Boye Tranum – Cyber Security Expert
Associate Director, Cyber Security

Simon Milford – Cyber Security Expert
Head of UK Cyber Security

Tony Xiang Zhao – Control Systems Engineer
Senior Electrical Engineer

Alasdair Cant – Dynamic Positioning Expert
Senior DP and Controls Engineer

Stephen Norman
Senior Business Development Manager UK & West Africa

Ajay Kumar
Marine Engineer

Ed Smith
Transport Risk Assessment

Insurance Market Representatives

Francis Lobo – Head of Upstream Oil & Gas Engineering – Canopius
JRC Cyber sub-committee Member
Report Author

James Miller – Head of Energy Engineering, Overseas General Insurance – Chubb
JRC Engineering sub-committee co-Chair

Stephen Hawkins – Global Product Head for Upstream Energy – XL Catlin
Underwriter

Alex Barnes – Head of Energy – Beazley Group
JRC Member
Underwriter

Chris Murlowski – Marine and Energy Executive – Performance Management
Lloyd's

James Straker-Nesbit – Senior Technical Executive - Lloyd's Market Association (LMA)
JRC Secretary

APPENDIX III.

Design Practices

Design Practices

This section describes the design practices related to hydrocarbon containment and facility protection systems at typical oil and gas facilities worldwide as these are pertinent to the discussions.

Oil and gas wells and facilities are located both onshore and offshore but from a systems perspective may be considered topologically synonymous. In the direction of hydrocarbon flow, the main process facilities in place are typically Wells, Well-site Facilities, In-field Lines, Central Processing Facilities, Offshore Storage, Export Pipelines, Onshore Oil Terminals & Storage Facilities, Onshore Gas Processing Plants, Gas Storage and Pipeline systems.

During the workshop, the worst MAH scenario possible was considered for each of these constituent parts, with onshore and offshore installations considered separately, as appropriate. The narratives below document the design practices assumed for each of these constituent parts that informed discussions at the workshop.

Wells

Production wells are designed to contain the highest possible pressure that could be delivered from the oil and/or gas reservoir which is being exploited together with consideration of artificial lift systems such as gas lift. Injection wells are designed to contain the highest pressure that the water injection pumps or gas compressors are capable of delivering into the well. These design criteria mean that it would be physically impossible for an errant operator or cyber attack to create a situation that compromises the mechanical integrity of the well.

Wells are equipped with valves to control or shut-in the well and some of these valves are remotely actuated and therefore connected to the ICS. However, design practices mean that no significant valves that have the potential to permit flow to the external environment are able to be actuated remotely and such operations require manual intervention at the well site. Some wells with wellheads at surface (platforms, TLPs, onshore wells, etc.) have remotely actuated annulus pressure regulation/relief devices but these are small-bore lines and the volumes that might be released would not be of any great consequence.

So, in summary with respect to wells, onshore or offshore, the design criteria mean that, in the operations phase, it would not be possible for a cyber attack to result in a major accident scenario. Of course, in a persistent targeted cyber attack, the maintaining open of certain critical safety valves (such as the SSSV) could contribute to its execution as, for upstream oil and gas facilities, the major inventories (inexhaustible in the time-frame of an incident) are contained in the reservoir, risers and pipeline systems and the absolute shutting in of these inventories is of paramount importance to avoid catastrophic loss.

Wells are most vulnerable to cyber attack during the drilling phase of the well. Rigs are increasingly equipped with monitoring and control systems, some of which, if interfered with in a cyber attack, could result in a blowout with catastrophic consequences. Rigs are, however, also equipped with Blowout Preventers (BOPs), which are designed to be operated from independent systems to the primary drilling operation control systems, although it is not inconceivable that a targeted cyber attack could gain control of both these systems at the same time for the execution of the attack to its conclusion.

Blowout Preventers are intended to be ‘fail-safe’ devices. This means that the device reverts to a safe condition in the event of breakdown or malfunction. Therefore, if a virus or bug compromised the BOP system, causing it to malfunction, it should act to secure the well in a safe manner. As the Macondo incident illustrated, BOP systems may have certain vulnerabilities but the key point is that the drilling system and the BOP system would have to be compromised in a precise manner, and sustained as such, for an attack to have a chance of being successful. As pressure control in the well is usually exercised by the mud column, the attack would have to compromise the physical barrier of the mud column – an intrinsically cyber safe barrier. This is considered extremely unlikely, certainly on a systemic basis.

A credible risk in the drilling phase relates to wells that are drilled from DP floating units. It is possible that a cyber attack can be perpetuated that drives these types of drilling units from over the well while still connected and operating. However, in the worst case of this scenario, weak points designed into the riser should cause it to fail above the Lower Marine Riser Package (LMRP). As this is above the BOP, the Blowout Preventers should shut-in the well as they are designed to automatically mechanically actuate in the event of such an occurrence. Assuming adequate well design, with sufficiently designed gas kick tolerances maintained during drilling operations, the event would be contained. In any case, in this scenario, the mud column would be a physical, intrinsically cyber safe barrier to prevent an event from occurring.

Major accident events arising from the wells inventory (drilling or operating) from a targeted attack are therefore considered highly unlikely to be successfully perpetrated and, similarly, the systemic risk associated with the ‘Wells’ constituent part of the upstream oil and gas process systems is considered to be extremely low with the current drilling technologies and design criteria/philosophies generally in use. This conclusion may not apply to well control techniques (MPD, UBD, etc.) where the mud column is not the primary barrier, and it is recommended that insurance markets capture appropriate information so the systemic exposures in this respect may be assessed and monitored.

Well-Site Facilities

For offshore facilities, well-site facilities may comprise subsea templates, manifolds, Pipeline End Manifolds (PLEMs), Pipeline End Terminations (PLETs), etc. Design practices mean that no significant valves that have the potential to permit flow to the external environment are able to be actuated remotely and such operations require manual intervention at the well site. These facilities are also designed to contain the maximum well or injection pressures (the shut-in well head pressure) that may be possible from the energy source (reservoir/pumps/compressors, etc.). Onshore well-site facilities follow similar design practices, and these design criteria mean that it would be physically impossible for an errant operator or cyber attack to create a situation that compromises these facilities to the external environment.

Novel, evolving subsea facilities such as subsea compression stations, etc. have not been addressed as, at the time of writing, they are currently not deployed extensively in oil and gas operations. It is recommended that these are reviewed on a case-by-case basis as, if it is possible that a cyber attack could release hydrocarbons to the external environment, environmental damage could be very severe, especially at locations where these facilities may be installed to deal with the freezing of the seas in winter. This is because a loss of containment (especially low level) may not be observed for a long time as escaping hydrocarbons could accumulate over time under the ice layer and only manifest when the ice thaws.

In-field Lines, Risers and Pipeline Systems

The lines with the greatest potential for major loss are the large diameter lines. Onshore, these lines are equipped with block stations and automatic instrumentation that isolate sections of the line in the event of a loss of containment. Block stations are typically located 20–30 miles apart but may be as close as 3 miles to each other, depending on assessed risk and consequence.

Pumping facilities can be used to over-pressure these lines, as occurred when the Baku-Tiblisi-Ceyhan pipeline in Turkey was caused to explode. Offshore deep-water pipelines that use high integrity protection systems are also vulnerable to cyber attack.

High Integrity Pressure Protection Systems (HIPPS) are used in oil and gas facility design to prevent over-pressurisation of facilities when a high pressure section of the installation is connected to a lower pressure section that requires protection. This minimises the use of relief systems that result in flaring or venting of hydrocarbons and hence is environmentally preferable. They are often also used to lower costs in plant design.

Inverted High Integrity Pressure Protection Systems (iHIPPS) are used to protect deep-water pipelines where water depth requires very thick-walled pipe to prevent the pipeline from collapsing due to external water pressure. With an iHIPPS, the pipeline wall thickness can be thinner as it needs to only cope with a differential pressure rather than an absolute pressure. When the internal pipeline pressure falls below a certain value, the iHIPPS shuts valves to trap pressure in the pipeline section, preventing further pressure drop and pipeline collapse. As iHIPPS typically operate over the entire deep-water section of the line (without intermediate block stations), a malfunction in the iHIPPS might result in collapse of the entire deep-water section of the line.

In-field lines typically do not contain any in-line valves and are rated for the highest pressure that they could encounter so it is unlikely for a cyber attack to physically compromise any of these lines.

Offshore Facilities (Fixed and Floating)

Offshore facilities typically comprise jacket structures with topsides that process production received from wells. They also have facilities that enable injection into wells or export lines, power generation facilities, various utilities, accommodation and sometimes include an oil storage capability. The jacket structure that forms the structural foundation, enabling process and other activities to take place, can be replaced by a floating unit, which is tethered to the sea bed with moorings or tendons. The narrative relating to process design applies equally to fixed and floating facilities, with the floating facilities including an additional aspect related to maintenance of its buoyancy which is addressed separately.

When production from the wells and subsea lines enters the process domain, there are specification breaks which permit transition from high to lower pressure, high to lower temperature and between corrosive and non-corrosive environments. With respect to pressure, over-pressurising of the lower pressure systems is managed by consideration of the full range of scenarios that could occur. After appropriate safety factors are applied conventionally, relief systems (Pressure Safety Valves (PSV) or PRV, rupture/bursting discs) are incorporated into the design. The relief system opens an alternative outlet for the fluids in the system once a set pressure is exceeded. The alternative outlet leads to a flare or venting system to safely dispose of the fluids, thereby not permitting the pressure to breach the design pressure of the lower pressure system.

In most offshore oil and gas facilities, any valves in the lines from relief valves, etc. to the flare or vent systems are manual and not connected to the Integrated Control and Safety System (ICSS). These valves may be required during commissioning and for maintenance activities and must be physically maintained open (either by plant operator routines or physically locking or securing open). A status register of these valves is usually also maintained.

It was therefore felt that static offshore process facilities (with the exception of HIPPS-protected systems) would be adequately protected by mechanical means on almost all offshore installations worldwide and the systemic risk from a cyber event would as a result be very low. However, this view was contested at the workshop and it is therefore recommended that further work seeks to identify the offshore installations not protected by such intrinsically cyber safe mechanical (or other) devices.

As mentioned earlier, HIPPS are increasingly being used to protect lower pressure systems from high upstream pressures. HIPPS are designed to detect the increasing pressure and rapidly shut off the high pressure before the design pressure of the lower pressure system is exceeded, thus preventing loss of containment through rupture (explosion) of a line or vessel.

Facilities with HIPPS may be vulnerable as they are instrumented (programmable), but the author is informed that HIPPS are independent of shutdown systems and have their own shut-in valves, independent logics and instrument sensing elements, normally only transmitting information regarding their status. This, however, was not corroborated by workshop participants and would need to be investigated further.

HIPPS used in offshore applications typically have a very high degree of safety and reliability, typically Safety Integrity Level (SIL) 3 or 4, due to the potentially large loss of life. The probability of failure on demand for SIL 3 systems is 1/1,000 to 1/10,000 and for SIL 4 is 1/10,000 to 1/100,000.

Conventional HIPPS rely on complex electronics and instrumentation and may have connections to the DCS (although these connections are reportedly ‘read only’). HIPPS tend to be individually designed for each application and so depending on the system architecture, the heavy reliance on electronics and instrumentation means that certain HIPPS may be vulnerable to cyber attack. Mechanical HIPPS are also available, which are designed to reduce the complexity of current HIPPS technology and provide a reliable subsea and topsides alternative to the current instrumented systems. These systems by their nature are not vulnerable to cyber attack and are intrinsically cyber safe.

Apart from these process design protections, offshore process facilities have fail-safe emergency shutdown (ESD) and blowdown systems adding preventative layers of protection and also F&G detection and firewater and deluge systems, which are a mitigating layer of protection to reduce the severity of an event if it occurs. The ESD and blowdown system takes automatic and independent (fail-safe) action to prevent a hazardous situation from developing.

Additionally, the inventories in offshore process facilities are relatively small (certainly compared to onshore occupancies such as refineries, tank farms, etc.) and typically capable of being evacuated from the facility (via blowdown) in less than 15 minutes and, together with the density of the detection and firewater systems designed into upstream facilities, the extent of damage is also mitigated.

In the past (older systems – pre 2010), F&G systems were stand-alone equipment or a hardwired mimic overview panel via relays. Mitigation of the risk would take place via automatic hardwired activation of control measures. Today, F&G detection systems are generally Programmable Electronic System (PES) type and tightly integrated with the overall process safety strategy in an ICSS. Mitigation takes place via the ESD system or directly from the F&G system itself. While pathways to the older systems are fewer, the security of these systems is typically not as high as the modern systems. Only fully pneumatic/hydraulic safety systems should be considered safe from cyber attack.

In older systems, if the process system were to be compromised and a loss of containment resulted, the F&G detection system would activate the ESD system, shutting in the incoming flows from the reservoir and also the pipelines and risers. Blowdown of any remaining process inventory would be completed within 15 minutes. It is expected that these actions would limit the potential damage to under the $100 million threshold. Concomitant control of both systems would therefore be required to affect a catastrophic loss scenario, which is considered unlikely except, perhaps, in a targeted cyber attack with significant knowledge of the systems being targeted.

In the post 2010 systems, the secure communication between the Human Machine Interface (HMI) layer and operational PLCs is done by deep packet inspection on the network communications between each PLC and the HMI layer by a rugged firewall. The firewall blocks any unauthorised communication for either control instructions being fed to the PLC or information being fed back to the HMI layer and generates alarms to inform the operator.

Communication from unknown devices on the HMI network is blocked by the firewall. In addition, deep packet inspection prevents the HMI from issuing commands or requesting data from registers that are not in the approved list configured in the firewall. This configuration provides assurance that the Modbus PLC communications are robust and resilient from unintended external interference.

The main industrial automation technical standard used internationally is IEC 62443, which requires separate network levels with defined zones, conduits and risk-assessed SILs.

The broad design criteria for equipment SIL is as follows:

SIL 1:	Protection against casual or co-incidental violation
SIL 2:	Protection against intentional violation using simple means
SIL 3:	Protection against intentional violation using sophisticated means
SIL 4:	Protection against intentional violation using sophisticated means with extended resources

While the conclusion from the above discussion pertains mainly to static process facilities, upstream facilities include rotating equipment and other facilities with a dynamic component. These usually have automated protective functions built into the machinery. These protective functions could be targeted and compromised with serious consequences. However, the overall platform F&G detection and ESD systems are designed to respond (irrespective of whether or not the cause was a cyber attack) if such an event occurs and avert catastrophic loss. As the protections (over-speed, etc.) for rotating/dynamic equipment are built into the equipment at manufacture, though, these can be compromised. The Stuxnet virus attack highlighted this vulnerability.

As the PD losses relating to an individual facility arising from such events are considered likely to be less than $100 million, these scenarios were not considered further at the workshop. It should be noted that such attacks might result in significant BI/LOPI losses and it is considered that these types of equipment are more vulnerable to cyber attack and also systemic effects. The systemic effects are potentially highly geared as, if much of this equipment is affected in the same incident around the world, then outage times (and consequently BI/LOPI) would be extended due to manufacturing facility limitations for this equipment. This entire area warrants further detailed examination in subsequent workshop(s).

Ballasting is extremely important to maintain the integrity of floating structures (semi-sub units, FPSOs, FLNGs, FSRUs, etc.). Imbalance created by improper ballasting (possibly resulting from a cyber attack) of semi-sub units could result in the facility tilting. However, these floating structures are designed such that, even if they were tilted to the maximum extent possible by ballasting operations, they would not overturn and capsize (except potentially in adverse weather).

With ‘ship shaped’ units, improper ballasting (or over-pressuring of tanks) during loading/unloading operations could cause failure of the hull and catastrophic loss. Over-pressuring of the hull would require physical intervention on-board to manually shut valves that connect the cargo tanks to the vent system and, therefore, creation of this catastrophic scenario by cyber attack alone may not be considered credible.

Ballasting operations on the other hand are more vulnerable to cyber attack. The operations are monitored on a computer system (Load-Master or equivalent) and tampering with the Hull Stress Monitoring System (HSMS) calculations, output or display/alarms, etc. could cause a scenario where the hull of the vessel fails. Ballasting, however, takes place over a long duration and certain specialists considered that mariners responsible use paper logs and perform independent physical checks against the vessel operations manual to verify indications from the computerised systems, hence, from a system’s viewpoint, an intrinsically cyber safe barrier may exist.

However, this view was not corroborated during workshop discussions, with the consensus view being that modern mariners are increasingly dispensing with the traditional checks performed and relying on automated or digitalised systems. Further investigation and proceeding on a case-by-case basis would be required to understand the extent of systemic risk in this important area.

DP Vessels

DP of vessels is used extensively in oil and gas operations from drilling rigs and pipe-lay vessels, to accommodation units and large maintenance vessels, which often dwarf the offshore platforms that they are working next to. The DP control system maintains the vessel’s position or precisely controls its movement by use of vectored thrust. The DP control system computes thrust and direction for each thruster to counteract the effects of wind, tidal current and wave motion. The calculation is based on information received from position reference systems and vessel sensors. The DP control system is also the subject of a detailed Failure Modes and Effects Analysis (FMEA) and frequent sea trials. Thrusters are also used to assist station keeping/orientation on some FPSOs, etc.

The scenario where the DP system could be used to drive a floating unit drilling off a well has been discussed in an earlier section. Another major accident scenario could arise if large maintenance vessels operating adjacent to offshore platforms could be triggered to drive off and strike the platform, causing its collapse or initiating a totally destructive event, as occurred at the Bombay High North (BHN) platform in the Arabian Sea. While the event was not cyber-related, it illustrates the scale of damage that can result from such an incident.

DP systems are equipped with analogue stops for each thruster, which can be manually activated on-board to stop the vessel. Automatic drive-off detection and shutdown may be available from some vendors, but it is possible that a cyber event could compromise the electronic position references, in fact, initiating the drive-off. There are numerous position reference systems of various types in use on a vessel working alongside a platform or Floating Production System (FPS). Several of Global Positioning System (GPS), Inertial Navigation System (INS), hydro acoustic, laser or radar would be in use and all 'in use' references would need to be compromised simultaneously. Attacking a single sensor type, such as GPS spoofing, would not be enough to cause drive-off. However, if a virus/worm or other malware spoofed an operator instruction to, say, move 50 metres to the north, the vessel would respond accordingly and the consequences would be similar to a drive-off.

Depending on design, emergency stops can be initiated locally at the thruster, from the Emergency Control Room (ECR) or from the vessel bridge. However, actuation in that case would rely on visual observation and it is felt that it is likely this observation would not be made until it was too late to avert a significant incident.

It should be mentioned that MAH scenarios during the project phases (fabrication, transportation and installation) were not addressed during the workshop as, while significant losses (above $100 million) consequent on a cyber-related event are possible, the absence of hydrocarbons in the facilities dramatically reduces the potential for physical and environmental damage. Also, as very few projects worldwide are in the same phase (installation phase being the most vulnerable) at the same time, the systemic risk that may be generated from related insurance policies would be low. In any event during critical phases of offshore installation activities, the vessels in use typically operate using DP and, as such, the worst case for the project phases would be the total loss of the adjacent asset and therefore 'Projects' may be considered in this systemic risk scenario.

Onshore Facilities and Storage

Onshore facilities (well-site and central processing facilities), oil terminals, tank farms and underground gas storage present a different cyber risk profile essentially, as the inventories of hydrocarbon that may be released are orders of magnitude greater than the inventories of hydrocarbon contained in a typical offshore process facility.

Some offshore facilities also have significant storage but these are typically in gravity-based structures underwater or in compartments in the hulls of FPSO, FLNG and FSRU offshore installations. In cases of compromise of storage, due to the inventories involved, it is considered that the $100 million threshold could be exceeded either due to the ensuing pollution event or catastrophic PD.

Gas storage facilities can similarly be compromised by cyber attack, causing over-pressurisation of the gas reservoir and breakdown of rocks and subsurface loss of containment. If these were to breach to surface, the resulting PD could easily exceed the $100 million threshold.

The above sub-sections describe upstream oil and gas design practices, and the conclusions in this report are based on an understanding of these physical considerations. However, it should be noted that, after facilities are put into service, degradation naturally occurs over time and sometimes to the extent that facilities are derated and operational procedures put in place to manage the increased risk. In such situations the above assumptions would be violated and these facilities could be more vulnerable to cyber attack than indicated by this report's conclusions. Any insurance framework put in place should seek to assess the state of the facilities in this respect while gathering data to consider the insurability of those facilities for cyber risk.

In a world evolving with increasingly Volatile, Uncertain, Complex and Ambiguous (VUCA) characteristics, it is more important than ever before that careful attention is paid to maintaining facilities to their original design. If changes are proposed that reduce the robustness or resilience incorporated by design (such as the derating of facilities), the implications for personnel safety and property/environmental damage that could occur consequent upon a cyber attack should be carefully analysed during the risk assessments performed.

APPENDIX IV.

Cyber Defences

This section briefly covers some of the current good practice practical measures being implemented to reduce risk related to cyber threats.

Organisational

- Implement a cyber security policy with top level management accountability.

- Implement organisational structures covering both IT and OT domains, with defined roles and responsibilities.

- Implement procedures including:
  - Disaster Recovery - including protocols for maintaining and checking backups
  - Access Control – including vetting procedures and Cyber Work Permits for external parties
  - Change management processes for all updates (including databases) and patching requirements
  - Disabling of USBs and other access modes (Wi-Fi, Bluetooth, etc.)
  - Procedures for mobile devices.

- Implement programmes to increase cyber security awareness among employees.

Physical

- Review system design with the aim of reducing cyber risk level to As Low as Reasonably Practicable (ALARP) using air-gapping, non-programmable software, unidirectional gateways, etc. depending on data transfer and remote control/access requirements.

- Aim to reduce connectivity between process control systems and safety systems to the maximum extent practicable and consider if unidirectional or encrypted transmissibility could offer a solution with the required benefits but without the drawbacks of increased cyber vulnerability.

- Review existing systems to assess exposure and vulnerabilities and determine if compliance to most recent ISA/IEC/IEEE standards is required.

- Perform CHAZOP studies of all ICS architectures to ensure sufficiency of system architecture and hierarchies.

- Review security-level agreements with peer sites, vendors, contractors and service providers, and perform appropriate verification and assurance.

- 'Sand-box' all equipment brought to industrial facilities and offshore installations.

Virtual

- Implement remote (trusted) access channels with appropriate security.

- Implement firewalls within an appropriate system architecture. It should be noted that, while these are important and necessary, these are not necessarily sufficient to adequately protect against cyber attack on IACS. Whitelist defences and smart-listing should be considered for defending ICS against unknown exploits.

- Implement IDS, preferably both signature-based detection and anomaly-based machine learning systems across the network and also within IACS system if isolated (or managed via unidirectional gateways).

Assurance

- Perform regular system audits (including security audits) – closeout findings.

- Perform security and vulnerability assessments.

- Apply Six Sigma Quality Function Deployment (QFD) to a modified 'Damage (Potential) Reproducibility Exploitability Affected (Users) Discoverability' (DREAD) model, or other, to quantify and prioritise vulnerabilities discovered during security testing. It is recommended that 'damage' should include facilities and the environment (and, if possible, business impact), the 'affected' should include facilities impacted, and the rating for 'discoverability' should be assumed to be the maximum rating unless there are compelling reasons for assuming a lower rating.

- Perform periodic onsite cyber security-related drills – implement findings.

- Routinely check disaster recovery processes (especially backup and restore). Backups should be in a secure location, offsite and/or in the cloud.

- Commission penetration testing to verify firewalls and IDS efficacy and vulnerability scans (except on operational ICS systems due to the risks to the operation. The primary goals of safety and reliability mean that, to perform adequate penetration testing, etc. in a safe manner, a dedicated non-production test environment should be utilised).

- Perform independent third party security assessments.

The following shows a simplified drawing of acceptable system architecture for process units (from Recommended Practice – DNV GL-RP-G108 Edition September 2017):

Figure 4-7 shows a simplified drawing of zones. In this figure, only two process zones (P and Pn) and two safety zones (S and Sn) are shown. P and S could e.g. be for a critical turbine system with a high security level, while Pn and Sn could be for a less critical sand-monitoring system with a low security level. The figure also shows examplesof conduits connecting the different zones.

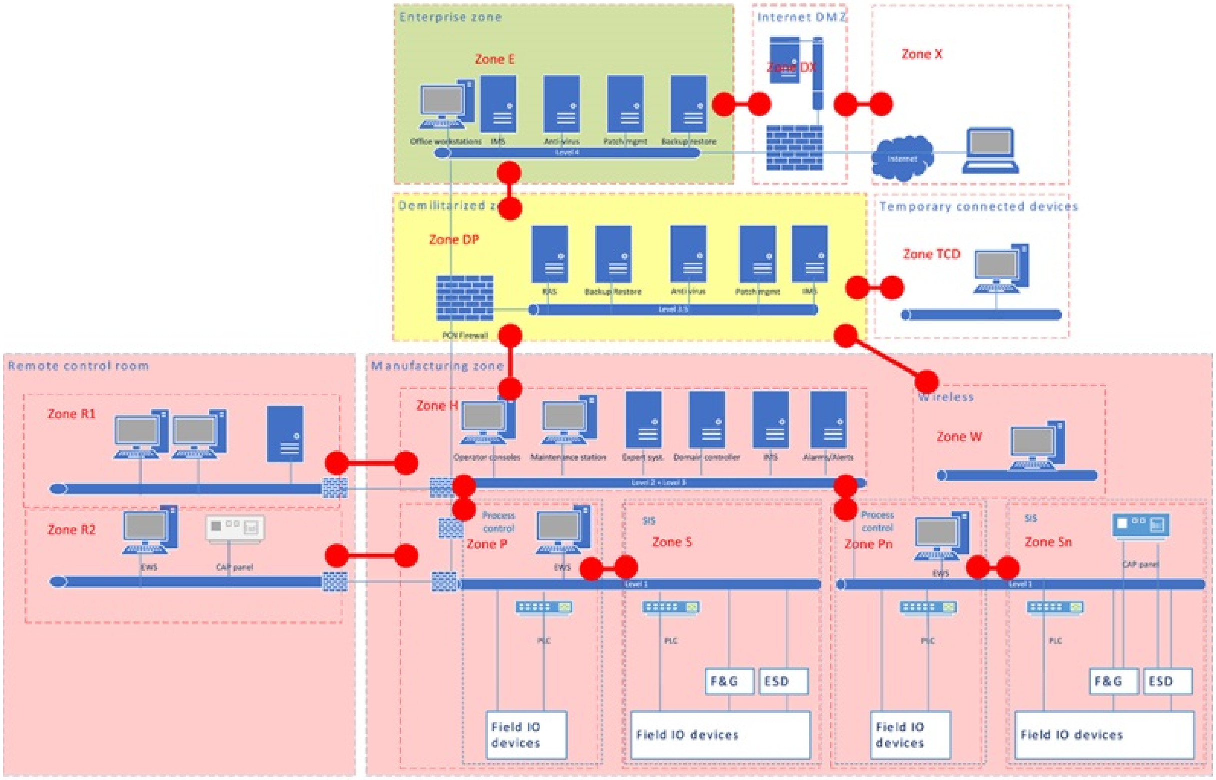


Figure 4-7 Example zone and conduit drawing

The DNVGL-RP-G108 recommended practice for cyber security in the oil and gas industry considers good practice covering all phases of an oil and gas development's life cycle, and adoption of this recommended practice should be encouraged to lower the risk related to cyber threats that may present at oil and gas installations.

It must be emphasised that this standard only partly addresses cyber risk in design, as one of the conclusions of the cyber workshop was that an alternative philosophic and holistic approach is necessary in the design of upstream oil and gas facilities to adequately address MAH scenarios that may arise as a result of cyber attack. In particular, engineering design processes should not place ultimate reliance on any non-intrinsically cyber safe instrumented or automated system while considering the design with respect to MAH scenarios.

Other guidance documents:

- NIS Directive (EU) 2016/1148
- HSE guidance on managing Industrial Automation and Control Systems (IACS)
- IEC 61511-2 :2016
- IEC 62443 interpretation = RP108 from DNV GL
- ISO 27001 - Note: Recommends independent verification that an organisation is compliant

APPENDIX V.

Acronyms

Acronyms

ABAP	Advanced Business Application Programming
ABB	ASEA Brown Boveri
ALARP	As Low As Reasonably Practicable
ATM	Automated Teller Machine
BHN	Bombay High North
BI	Business Interruption
BOP	Blowout Preventer
BP	British Petroleum
CABBE	Cyber Attack Buy Back Endorsement
CHAZOP	Control Hazards and Operability Study
CMZ	Classified Militarised Zone
DCS	Distributed Control System
DMZ	Demilitarised Zone
DNV GL	Det Norske Veritas Germanischer Lloyd
DP	Dynamic Positioning
DREAD	Damage (Potential) Reproducibility Exploitability Affected (Users) Discoverability
EAM/PM	Enterprise Asset Management/Plant Maintenance
EBS	E-Business Suite
ECR	Emergency Control Room
ESD	Emergency Shutdown
F&E	Fire and Explosion
F&G	Fire and Gas
FLNG	Floating Liquefied Natural Gas
FMEA	Failure Modes and Effects Analysis
FPS	Floating Production System
FPSO	Floating Production Storage and Offloading
FSRU	Floating Storage and Regasification Unit
GPS	Global Positioning System
HANA	High-speed Analytical Appliance
HIPPS	High Integrity Pressure Protection System
HMI	Human Machine Interface
HSMS	Hull Stress Monitoring System
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
ICSS	Integrated Control and Safety System
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
iHIPPS	inverted High Integrity Pressure Protection System
INS	Inertial Navigation System
ISA	International Society of Automation
IT	Information Technology
J2EE	Java 2 (platform) Enterprise Edition
JDE	JD Edwards
JRC	Joint Rig Committee
LMRP	Lower Marine Riser Package
LOPI	Loss of Production Income

MAH	Major Accident Hazard
MOC	Management of Change
MPD	Managed Pressure Drilling
NOC	Networks Operations Centre
OPC	Object linking and embedding for Process Control
OT	Operations Technology
PD	Physical Damage
PES	Programmable Electronic System
PLC	Programmable Logic Controller
PLEM	Pipeline End Manifold
PLET	Pipeline End Termination
PRV	Pressure Relief Valve
PSV	Pressure Safety Valve
QFD	Quality Function Deployment
RDS	Realistic Disaster Scenario
SAP	Systems Applications and Products
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SOR	Statement of Requirements
SQL	Sequence Query Logic
SSSV	Subsurface Safety Valve
TCP/IP	Transmission Control Protocol/Internet Protocol
TLP	Tension Leg Platform
UBD	Underbalanced Drilling
UOM	Upstream Operations Management
USB	Universal Serial Bus
VUCA	Volatile, Uncertain, Complex and Ambiguous