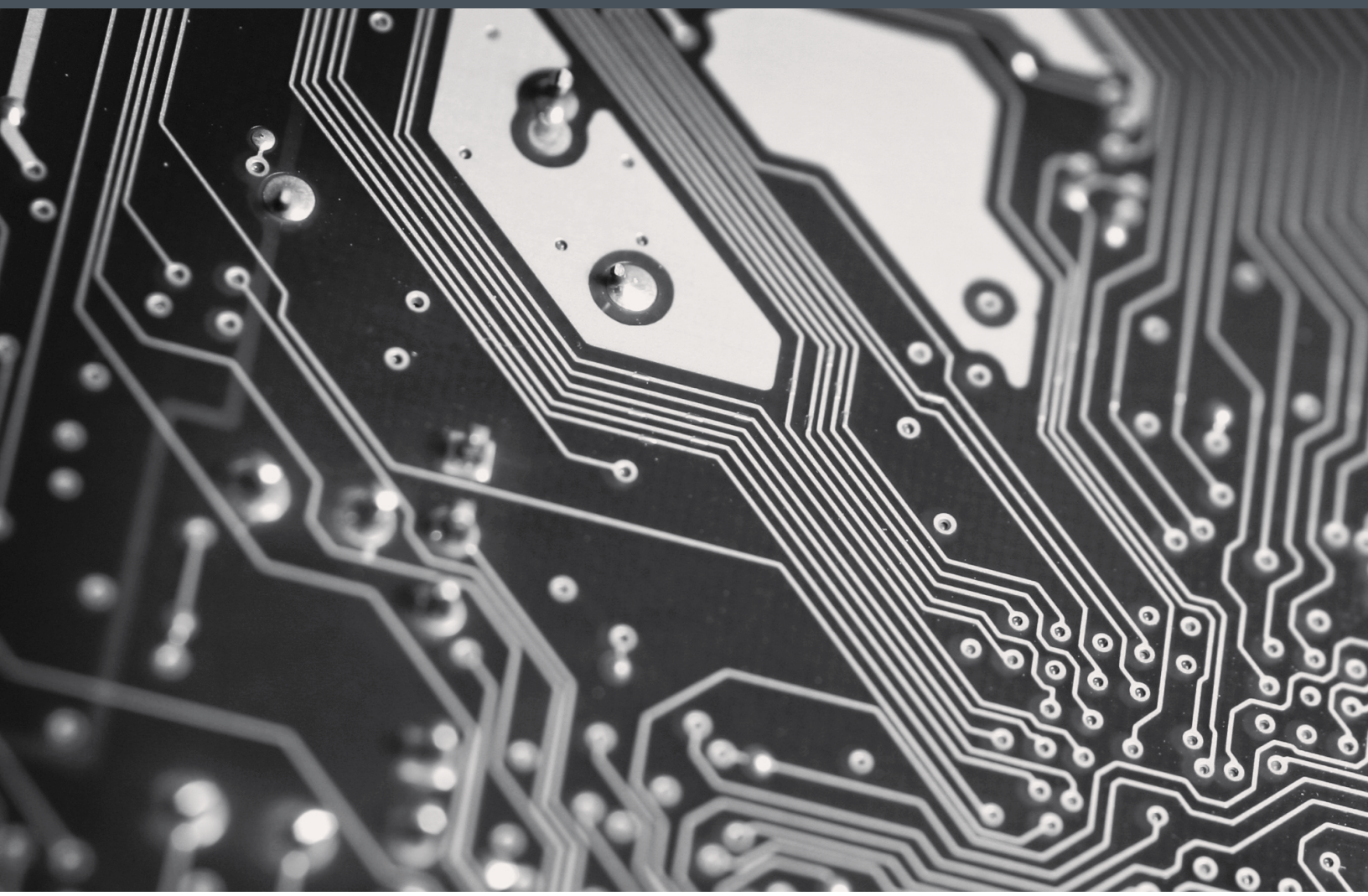

# ASSESSING AND ALLOCATING RISKS FOR DIGITAL TECHNOLOGY IN THE UPSTREAM E&P SECTOR

**"The robots aren't coming, they are already here."[1]**

**In May 2019, the Journal of Petroleum Technology addressed the exponential growth of digitized processes in upstream oil and gas operations. The Journal cited to Roger Jenkins, Murphy Oil's President and CEO, who stated, "[T]he adoption of digital technologies will continue to improve offshore operations, including improved well efficiency, real-time directional drilling, lower maintenance costs and safer operations."[2]**

1 What to Do When Machines Do Everything: How to Get Ahead in a World of AI, Algorithms, Bots and Big Data; Frank, M., 2017.

2 Digitalization is Changing Offshore Operations, Journal of Petroleum Technology, 6 May 2019, Donnelly, J.

Energy industry advisors at EY reported that a recent survey confirmed that the primary motivation to invest in digital technology was to improve operational efficiencies[3]. Artificial intelligence (AI) is creating significant improvements in real-time drilling data analyses. Industry projects are exploring the applications of AI to "provide improved warning time to critical situations by analyzing real-time data coming from the drilling operation" and using "digital twin models with real-time integrity data and deep analytical models to better assess the overall status of the drill fig and systems."[4]

Although the upstream energy sector may not have embraced digitized technology as quickly as other industries, the energy sector is rapidly increasing its utilization of digitized processes to reduce costs, increase efficiencies and improve safety. How operators, contractors, service companies and original equipment manufacturers are contractually allocating the significant risks inherent in the use of these digitized processes, is much less clear.

## Assessing and Allocating Risk of New Technology

### Assessment

How do you assess risks in emerging technologies? One of the principal obligations of corporate management is to assess both operational and financial risks. The utilization of new digitized processes will require the use of specialized skills to understand and assess the benefits and detriments inherent in these process applications[5].

The ability to assess risk is particularly important with regard to recognizing evolving cyber risks and exposures that accompany new technologies. These risks can include:

- Inaccurate or unreliable processes;
- Unauthorized access to, or use of, data;
- The use of third party contractors/ service providers; and
- Cybersecurity risks and the introduction of malicious viruses[6].

### Identifying Cyber Risks in Real Time

The U.S. Department of Homeland Security created the Cybersecurity and Infrastructure Security Agency (CISA) to assess cyber threats and enhance the industry's ability to defend against them. The CISA offers Alerts, which provide real-time updates about existing security issues, vulnerabilities and exploits, as well as Bulletins to address new vulnerabilities and the means to patch them.

### Determining Appropriate Risk Management Methodologies

The U.S. government has also developed analytic frameworks to assess risks inherent in digitized technologies through the National Institute of Standards and Technology (NIST), an entity of the U.S. Department of Commerce. NIST has developed a Cybersecurity Framework and Risk Management Framework (RMF), as well as guidelines for the application of the RMF to processes and systems. NIST standards used in the assessment of risks in upstream operations include:

- NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations;
- NIST 800-82 – Guide to Industrial Control Systems.

In addition, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA) have all developed similar risk assessment standards, which often overlap. For example:

- ISO/IEC 27001 is an international standard that internal and external parties use to assess a company's information security requirements. To provide a more "real world" context, ISO/IEC 27001 can control:
  - Information security policies;
  - Asset management;
  - Access control;
  - Operational security;
  - Communications security;
  - System acquisition, development and maintenance; and
  - Compliance.
- ISA 99 addresses industrial automation and control systems and has been utilized to create multiple IEC 62443 standards that also address control systems.

From a regulatory perspective, the U.S. Coast Guard (USCG) has created a Cybersecurity Framework for Offshore Operations, with categories, subcategories and mission objectives to make operations more secure. The mission objectives range from maintaining personnel safety (Mission Objective 1) to cyber situational awareness to understand and assess cyber threats and vulnerabilities (Mission Objective 5). This USCG Cybersecurity Framework provides regulatory context and reference points for industry operations and the contracts that support these operations.

Recently, contracts for the provision of digitized products and services in the upstream E&P sector have begun to reference these standards as foundational methodologies to assess the adequacy of information security and critical control systems. Although industry contracting practices are beginning to recognize the importance of baseline security assessments for the use of digitized systems, these same contracts often fail to adequately allocate liabilities and exposures arising from these same systems.

3 Oil and Gas Digital Investment Set to Surge as Efficiency Drive Intensifies; EY Press Release, 2 January 2019; Curtis, M.

4 Artificial Intelligence Improves Real-Time Drilling Data Analysis; Offshore, 2 January 2019; Evensen, O. and Haaland, O.

5 Emerging Technologies, Risk and the Auditor's Focus, Lindsay, J.B., Doutt, A. and Ide C., Center for Audit Quality, Harvard Law School Forum on Corporate Governance and Financial Regulation; 8 July 2019.

6 Id, at FN 8.

## Allocation of Risks Arising from Digitized Information and Control Systems

### Contractual Risk Allocation

For decades, the upstream industry has used contractual terms to allocate, limit and define liabilities between operators, contractors and service companies. Service contracts and bridging documents are often the documents that address these issues. For the context of this analysis, service contracts often provide terms in a "macro" sense, which can apply to various projects, services and locations around the world. On the other hand, bridging documents are often more focused on a particular application involving specific locations or operations.

With respect to service contracts, parties frequently use the following types of terms to allocate and/or limit risks of various types and magnitudes:

- Warranties regarding work, equipment and personnel;
- Key performance indicators;
- Performance of Work/Due Diligence/Good Oilfield Practice;
- Enforceable indemnity agreements;
- Insurance coverage in support of, or in addition to, contractual indemnities;
- Limitations of liability; and
- Force majeure.

These terms allocate risks ranging from delayed performance and daily rates to bodily injury, death, pollution and catastrophic loss that emanate from more traditional risks, such as loss of well control. So, why are companies not contractually allocating the significant exposures that could arise from failed digitized processes and/or cyber risks? The loss of critical control systems in various upstream applications could result in similar types of exposures addressed by traditional contractual allocation terms.

In part, the answer may be that the type of risks inherent in digitized processes and critical control systems are not as predictable as the more "traditional" exposures that have been allocated in decades of contractual forms. The nature of cyber risks is ever-changing and capable of creating catastrophic damages in certain applications, such as a high-temperature/high-pressure sensor on a deepwater export riser. The rapid development and application of digitized processes and controls has been accompanied by equally evolving cyber threats; creating a challenging environment to ring fence through risk allocation.

Although difficult, allocating risks for developing processes and exposures is not impossible. Contracts must adapt to the industrial environment that they serve, even when the evolution of the industry moves rapidly. For example:

- Warranties and performance obligations can utilize industry standards from the ISO, IEC and the ISA, as well as NIST guidelines and mission objectives from the USCG Framework. These reference points may be the new digital "Acceptable Oilfield Practices."
- Key performance indicators can similarly address obligations and requirements to update digitized processes and security measures to tackle the evolving threats identified by the CISA.
- Limitation of liability clauses must focus on the particular process and the impacts that could result from a misapplication of the process or introduction of a malicious virus.
- The scope of original equipment manufacturer obligations must be reasonably tailored to the scope of the project and the reasonably anticipated results from equipment or process failure.

## Insurance Coverage – What is Cyber Insurance?

Any compressive risk program in the upstream sector must engage a combination of contractual risk allocation and insurance. The vast majority of "cyber insurance" in London and domestic markets focus on response and remediation from a cyber-attack related to commercial, retail and financial industries. Most cyber policies are very limited with respect to property damage, bodily injury/death and pollution exposure.

The traditional liability, property and control of well coverages are tailored to exposures faced by companies in the upstream sector. Most of these policies contain exclusions for cyber related exposures. The insurance industry is gravely concerned about the extraordinary risks that could result from "systemic" cyber-attacks involving multiple facilities, wells, infrastructures, such as pipelines, power grids and commercial ports.

For the last 15 years, the London insurance market has relied upon the Institute Cyber Attack Exclusion Clause - CL 380 10/11/2003 (CL 380 exclusion) to avoid coverage for exposures arising from cyber related events. In July 2019, the Lloyd's Joint Rig Committee released the CL 380 Buyback Endorsement. This endorsement addresses damage to upstream and midstream facilities, including:

- fixed Offshore platforms or Offshore platform complexes and the subsea infrastructure for those platforms or platform complexes and physically connected wells within a one (1) kilometer horizontal radius;
- floating and/or mobile Offshore units and the subsea infrastructures for those units and physically connected wells within a one (1) kilometer horizontal radius;
- subsea infrastructures and physically connected wells within a one (1) kilometer horizontal radius;
- single pipeline Offshore and/or Onshore;
- onshore well site properties and wells within a one (1) kilometer horizontal radius; or
- other Onshore explorations and production property

The CL 380 Buyback Endorsement involves significant limitations/ exclusions and additional premiums.

## Contractual Risk Allocation and Insurance Coverage for Upstream Digitized Processes – the Path Forward

Although the evolution of digitized processes and the accompanying cyber risks may appear daunting, the energy sector is addressing these exposures in a proactive manner. Major operators and contractors realize the necessity of utilizing digitized processes to increase efficiencies, reduce costs and boost shareholder value. Risk assessment and allocation programs must continually adapt to new industry developments and not be guilty of linear thought processes when evaluating potential exposures.

On October 8-9, 2019, the International Association of Drilling Contractors (IADC) is presenting the Cybersecurity for Drilling Assets Conference in Houston, Texas. The Conference involves speakers from Chevron, ExxonMobil, Valaris, Diamond Offshore Drilling, Nabors, Helmerich & Payne, Cameron, Stena Drilling, RigNet, U.S. Coast Guard, ONG-ISAC and Palo Alto Networks. The Conference will address risk allocation in service contracts and bridging documents.

To view the IADC Cybersecurity for Drilling Assets Conference please visit http://www.iadc.org/event/iadc-cybersecurity-drilling-assets-conference/

Should you have any questions concerning risk allocation and insurance coverage related to the increased use of digitized processes in the upstream sector, please do not hesitate to contact the HFW USA attorneys listed below:


**GLENN LEGGE**
Partner, Houston
**T** +1 (713) 706 1941
**E** glenn.legge@hfw.com

**THOMAS LIGHTSEY**
Of Counsel
**T** +1 (713) 706 1952
**E** tom.lightsey@hfw.com

**CADE WHITE**
Senior Associate
**T** +1 (713) 706 4907
**E** cade.white@hfw.com

**COURTNEY CAMPION**
Associate
**T** +1 (713) 706 4901
**E** courtney.campion@hfw.com


**HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our energy capabilities, please visit www.hfw.com/Energy**

hfw.com



Americas | Europe | Middle East | Asia Pacific