International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Title: Digitalization

Problem Statement:

The petroleum industry is becoming increasingly dependent on digital systems, and the companies have ambitious plans for increased use of digital technology – along the entire value chain. Increased levels of digitalization present major opportunities for efficiency in the oil and gas industry and can also contribute to enhanced levels of resilience to major accident hazards. At the same time, new risks become apparent. The role of the human changes and -as a result- conscious effort is needed to make sure these risks are managed.

Digitalization involves the introduction of digital technology, such as computer engineering methods and tools, to replace, streamline or automate manual and physical tasks. This means increased use of integrated operations, remote operations, automatization, robot technology, artificial intelligence (AI) and access to computer resources and data visualization in order to analyze large volumes of data. Furthermore, digitalization initiatives in the industry will bring about change in the way companies work, both within the individual companies' own operations and organization, but also the implementation of new forms of collaboration and business models.

On one hand, this development can produce more efficient work processes, replacing manual labour, yielding better analyses and improved decision-making, with benefits for health, safety and the environment (HSE). On the other, there is also a need for the industry leaders to understand how this development may also introduce new risks and challenges. For example, with increased use of standard IT equipment and solutions in the industrial automation segment, cyber security becomes a relevant challenge within the industrial Information and Communication Technology (ICT) domain.

The industry will in many cases continue to use systems where personnel have an important role. In workplaces where automated systems are increasingly applied, operators' roles are changing. Examples of this may be; a driller who's work changes from manually adjusting drill bit rotation and fluid flow, to monitor and being ready to intervene if the automated drilling process fails; a maintenance engineer who has replaced his task of gathering data in field through, vision, hearing, smell, manual measurements and calculations – with evaluating a prognosis of time to failure based on a machine learning system presented in a dashboard; or a network security operator that instead of reviewing alerts and analyzing traffic data supervises an automated intrusion detection and response system. The change in operator role represents both a relevant cyber security and safety challenge within the industrial ICT domain and system interfaces.

Most operator errors arise from a mismatch between the properties of the system as a whole and the characteristics of human information processing. Unforeseen circumstances that cause the systems to deviate can be caused by malfunction of systems, the interfaces between systems, deliberate cyber-attacks or be a result of cyber collateral damage.

When developing and implementing automated system designers risk creating a work situation in which many of the normally adaptive characteristics of humans' natural problem-solving responses are transformed into dangerous

liabilities. The system must have the ability to provide information to the operator about its actions and reasoning. As such, data models and interfaces must be transparent and explainable to the human operator.

Guidance and standards on design of software solutions, ICT security and HF methods exist. However, holistic approaches and sufficient emphasis on cross-functional application, and technology that supports human performance, is often lacking. This leads to suboptimal solutions that depend on detailed and continuous update of standards as well as expensive and time-consuming training.

The changes we expect to see:

For the industry to promote human performance, reduce risk and prevent future incidents, the following priorities are expected to make a positive contribution:

- Increased industry attention and knowledge about HSE consequences of increased use of digital technologies.
- Managing risks and vulnerabilities related to digital technologies with an integrated perspective that includes human, technological and organizational aspects.
- Increased application of cross-functional standards and best practices with development of new guidance where gaps exist.
- Inclusion of design practices that increase safety in software solutions through system design that drives human performance. Further development of standards that reflect current challenges.
- Increased focus on learning initiatives targeting designers, operators and leaders for successful implementation of automated systems and digital technology.
- More systematic sharing and application of learnings from successful cross-functional collaboration related to the development and use of digital technology.
- Increased focus on human factors in cybersecurity.

External Organization(s) that could be tasked with leading the change / developing the solution:

- International Association of Oil and Gas Producers (IOGP) / International Association of Drilling Contractors (IADC)

Key performance indicators:

- Active sharing of experiences and lessons learned from successful implementations
- Topic clearly reflected in relevant sub-committees priorities / program
- Joint IRF/IOGP/IADC implementation

Owner: PSA

Date: October 2022