International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Digitalisation Problem Statement – Briefing Pack

October 2022

International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Which Problems are being tackled

International Regulators' Forum
GLOBAL OFFSHORE SAFETY

IRF and industry have prepared the following 3 problem statements to be addressed collaboratively

Prevention of well control incidents

- Greater emphasis on "left hand side" of well control bow-tie, particularly with regards to PPFG prediction and monitoring
- IRF contact: NOPSEMA (Australia)

Investigation quality / sharing & application of learnings

- Improve investigation quality and improve ways to embed learnings
- IRF contact: ANP (Brazil)

Digitalisation

- Reducing risks from automated systems with a human-centered design approach
- IRF contact: PSA (Norway)

Background

International Regulators' Forum
GLOBAL OFFSHORE SAFETY

The petroleum industry is becoming increasingly dependent on automated systems, and the companies have ambitious plans for increased use of digital technology. Complex integration of systems increases risk and ramifications for malfunctions that may cause serious incidents. Unforeseen circumstances causing systems to deviate can be malfunction of systems, interfaces between system components, deliberate cyber-attacks or plant upset as a result of cyber-collateral damage.

IRF first communicated this problem to IOGP & IADC in the form of an "IRF Problem Statement". The problem was refined and is currently being actioned by IOGP-led task force.

The purpose of this briefing pack is to share the problem statement and how it is being actioned with IRF members.

International Association of Oil & Gas Producers

Examples of the technologies and problems

Experiences and lessons learned from industries emphasize the criticality of the interface between human-automated systems for ensuring safe operations. Some examples on critical factors are:

- Situational awareness and meaningful control amongst those involved at the sharp end
- Design that supports human natural abilities when developing and implementing automated systems
- Targeted training and practice
- Reporting of automation errors as driver for (un)justified level of trust

"We saw in these two accidents that the crews did not react in the ways Boeing and the FAA assumed they would," (NTSB 737 MAX)

The same measures that make a system safe and predictable may introduce restrictions on cognition, which over time, inhibit or erode the disturbance handling capability of the actors involved (AF-447, Oliver et.al 2017)

* Endsley, 2017, SINTEF, 2020; NTSB Price, 2019; DSA, 2019

Evolution

2019

Kick off (Hague)

Follow up conversations IOGP/NOPSEMA (Sydney)

Initial PS drafted

2020

Follow up IRF meeting and IOGP/IADC input to IRF October

Decision to refine PS with more specific focus

Various activities in IOGP and continued IADC committee efforts

2021

Kick off framing meeting with IRF/IADC/IOGP. Feb 2021

New version of PS drafted incorporating feedback from IRF members, IOGP and IADC

Follow up meetings IOGP, IADC and IRF

PS published on IRFs webpages

2022

IRF Digitalization workforce established (HSE UK, ANP, CNLOPB, BSEE, PSA)

Regular meeting with IRF / IOGP / IADC

New version based on input from IOGP / IADC

Joint communication (ONS22, IADC Amsterdam and Oslo)

Identification of relevant sub-committees in IOGP and IADC

Digitalisation Problem Statement

Problem statement:

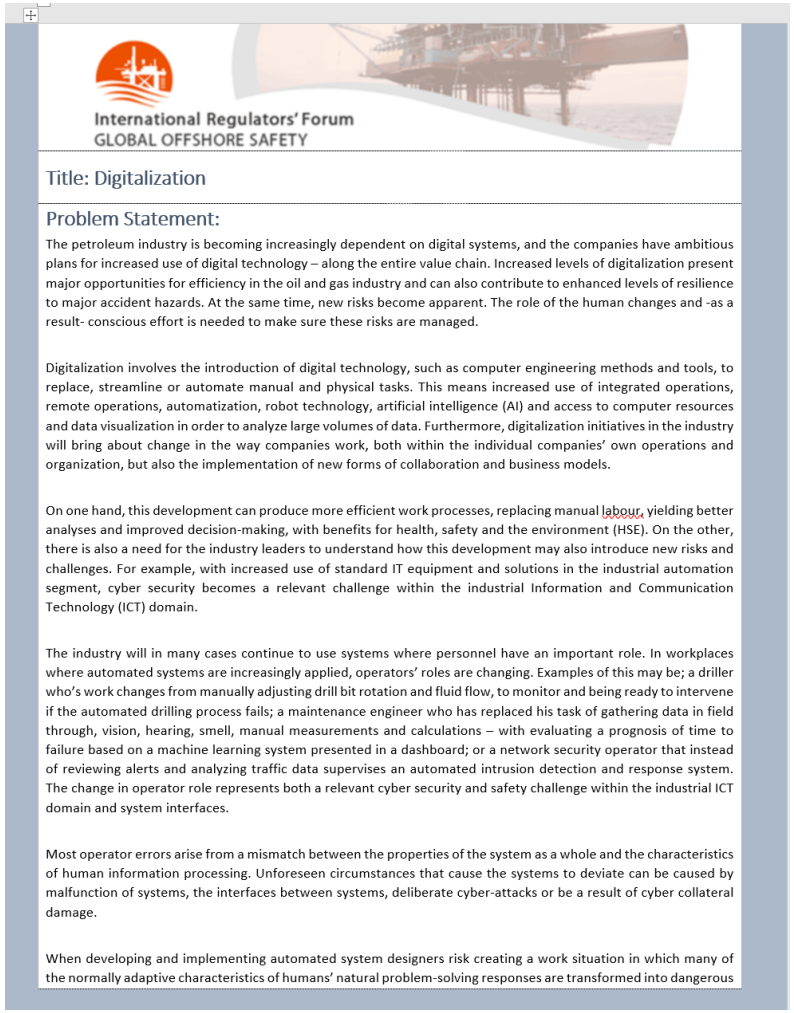
- Greater emphasis on design that supports human natural abilities when developing and implementing digital and automated systems

Expected outcomes:

- 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.
- 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.

Deliverables/KPIs:

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



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

Organisation and reporting

- IRF working group. Reports to:
  - IRF management committee (3 monthly)
  - Entire IRF (twice per year)

- IADC:
  - Nominate committees to engage
  - Identify and plan deliverables

- IOGP:
  - Nominate committees to engage
  - Identify and plan deliverables

- Other industry bodies and standards organizations to be engaged at a later stage

Forward Plan

Activities	2021	2022	2023
Prepare briefing pack (IRF) and present PS in IRF Mid-year meeting			
Establish extended IRF work group			
Regular IRF/IADC/IOGP meetings			
Establish joint IRF/IADC/IOGP comms/outreach			
Decision if any further concrete deliverables are needed and next steps			
Execute joint communications plan for aligned message			
Joint IRF work group meetings			
Decide any future work scope			
Continue dialog with relevant IOGP and IADC sub-committee Continue experience transfer in the IRF oversight workforce on issues such as cyber security and digital initiatives in a HTO perspective in the petroleum			

International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Digitalisation Problem Statement – Briefing Pack

October 2022

International Regulators' Forum
GLOBAL OFFSHORE SAFETY