International Regulators' Forum
GLOBAL OFFSHORE SAFETY

Title: Digitilization

Problem Statement:

Despite increased automation, the industry will in many cases use systems where personnel have an important role. In workplaces where automated systems are increasingly applied, operators' roles are changing. This change in operator role also represents a relevant cyber security 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.

When designing and implementing automated system designers risk creating a work situation in which many of the) (its natural heuristics and biases) are transformed into dangerous liabilities.

Because of human operator's innate powers of knowledge-based reasoning (normally adaptive characteristics of human cognition) to cope with system emergencies the industry will continue to have humans in the loop. 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. Most hazardous situations arise due to a discrepancy between the properties of the system as a whole and the characteristics of operators information processing. When developing and implementing automated systems (software solutions for process automation, and cyber protection systems), research and experience show that insufficient emphasis is put on consequences for human ability to monitor, detect, safely intervene in order to manage and mitigate hazardous situations.

System designers may unintentionally create a work situation in which many of the normally adaptive characteristics of humans' natural problem-solving techniques are transformed into dangerous liabilities. In order to promote the development and implementation of reliable and robust digital solutions it is important to be aware of and understand how this development might introduce new types of risks. Understanding the operator's role in hazardous events and incident response of critical chain of events is crucial for achieving in-depth security. Increased automation and thus complexity of systems leads to increased demands for continuously updated knowledge and expertise for system designers, key stakeholders and leaders.

Guidance and standards on design of software solutions, ICT security and HF methods exist. However, holistic approach and sufficient emphasis on cross-functional application, and technology that supports innate characteristics of human cognition, is often lacking. This leads to suboptimal solutions that highly depends on detailed and continuous update of standards as well as expensive and time-consuming training. Therefore, we believe there is opportunity to:

- Better prevent and safely manage hazardous events and incident response in order to achieve in-depth security, including cyber security protocols, to support guidance and standards for the development;

- Better incorporation of human centred approaches in the introduction of digital technologies;
- Better detection and management of human – automation risks in digital solutions across industry;
- Improvement of cross-functional perspective in development and use of automated systems in the industry; and
- More systematic sharing and application of learnings from successful cross-functional collaboration related to the development and use of automated solutions / digital solutions.

The changes we expect to see:

In order for the industry to promote human performance through human centred technology, reduce risk and prevent future incidents, the following priorities are expected to make a positive contribution:

1. Identification and resolution of any roadblocks within the industry hindering a cross functional approach in systems engineering (human-centred technology development).
2. A move towards structural inclusion of human-centred design, thus enabling human performance imperatives to be fulfilled, especially in compromised situations including cyber incidents.
3. Increased focus on strengthening designers, operators and leaders competence and expertise on how to design and implement technology that supports normally adaptive characteristics of human cognition.
4. More active sharing of experiences and lessons learned from successful implementations, including how to promote human-centred and cross functional perspective in technology development projects and subsequent application and implementation of those learnings.
5. More systematic generation and application of use cases for applying human factors in system engineering, shared across the industry and communicated throughout operator organizations.
6. Clearer priorities on Human Performance, both through work culture and the promotion of human-centred technology development, thus increasing operational cyber resilience.

Industry Association(s) invited to lead the change / develop the solution:

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

Key performance indicators:

- Increased application of cross-functional standards and best practices with development of new guidance where gaps exist.
- Increased focus on learning initiatives targeting designers, operators and leaders for successful implementation of automated systems and digital technology.
- Increased cross functional corporation between agencies and industry organisations.
- Increased cross functional approach to technology development, promoting human-automation interface in digital solutions.
- Human-centred technology development clearly represented as a topic in industry conferences.
- Fraction of human-automation interface properties identified as threats and opportunities (including cyber security) in technology projects.
- Better alignment on above priorities across the various trade associations and entities who progress such areas.

Contact: Petroleum Safety Authority (Norway) Date: 25 June 2021
Endorsed by IRF Management Committee