**Project title: MAS – Meaningful Human Control of digitalization in safety critical systems**

The MAS project is about design of meaningful Human Control of digitalization in safety critical systems and supports the area "Knowledge-building Project for Industry" - PETROMAKS 2.

## Relevance to the call - Knowledge-building Project for Industry - PETROMAKS 2

This proposal is initiated by the oil and gas industry in Norway and Canada, which have seen the need to focus on safety and human involvement as digitalization is increasingly introduced in the industry. Key themes in digitalization covered in this project proposal are automation and remote operations. Digitalization may cause disasters if human factors (HF) are not sufficiently considered during design and operation. MAS is in line with this initiative and aims to increase safety, efficiency, and productivity in critical operations, with meaningful human control when needed. To ensure a safe, efficient and productive digitalization of the operation, there is a need to increase "meaningful human control", (Mecacci et al., 2019; Hagenzieker 2020; Santoni de Sio et al., 2018; Hoem et al., 2020). By meaningful human control we mean the ability of the whole system to provide the operators with relevant information, knowledge, and possibilities to safely control and monitor the operation during all conditions, including unanticipated events and failures i.e. all within limits of human abilities and possibilities. Meaningful human control requires best practices from the science of HF are used from the start (Lee et al., 2017). To mind the gap between "work as done" vs. "work as imagined" (Hollnagel, 2015), verification and validation (V&V) of organisation, tecnology and HF is needed. We base V&V on the often used CRIOP method, Aas et al (2009).

The MAS project supports area 5 of the Petromaks 2 program: Major accidents and the work environment. There is also a secondary support of area 3: Drilling, completions and intervention. The project will address offshore energy systems, and functions such as increased degree of joint operation and remote control. MAS combines the following cross-cutting activities: 1) Digitalization – through both automated and remote operations, and 2) challenges related to the introduction and use of new technology, by shedding light on the need for user centric design to support meaningful human control. The focus in these cross-cutting activities is on operations that require human interventions, e.g. drilling, process control, the operation of energy systems such as wind turbines, or in new types of automated operations (shipping on and below the surface, drones). The level of automation in these operations varies from human control to full autonomy, as described in SAE (2018). The results of MAS will provide design and operational guidelines that account for meaningful human control in operations that are highly digitalized (i.e., higher level of automation and/or remotely operated). The knowledge and methods developed can play an important role in technology qualification to be used in the oil & gas as well as other safety critical industries.

The project will support a joint Norwegian-Canadian collaboration effort to improve methods addressing human factors through the CRIOP method. The Research Council in Canada has approved a project – "Critical Intervention and Operability Analysis for Digital Ocean Operations (CRIOP-DO)", where Equinor, SINTEF and the HFC-network in Norway are collaborators. MAS and CRIOP-Do will provide a roadmap for a new wave of international collaborative, multidisciplinary research on risk, safety and human factors within major industrial operations undergoing digital transformation. MAS also supports the BRU initiative, Remote operations and future operating models, BRU21 (2020).

## 1. Excellence

The Norwegian petroleum sector has a world class (HSE) health, safety and environment level and has been in the forefront of implementing new safe technology and focus on a risk based regulatory regime based on tri-party collaboration between industry, regulators and the workforce. The strategic aim of the industry and regulators is for Norway to have the highest safety level in the world, and this aim is supported by MAS when automation and remote operations are implemented. The safety perspective and the tri-party collaboration can give Norwegian industry a strategic competitive advantage internationally related to exporting new safe technologies, regulatory practices, and methodologies supporting users. The project will build on the substantial collaboration from industry, regulators and human factors experts.

## 1.1 State of the art, knowledge needs and project objectives

There is a strong technology optimism related to digitalization as seen by several pilot projects. However, there are still challenges to address related to meaningful human control. Research and collaboration with industry and regulators (i.e. Petroleum Safety Authority-PSA) in the Norwegian petroleum industry, have identified several challenges (C) in the implementation of innovative digitalization (PSA, 2020):

- C1: The user observed that they some times do not understand what is going on behind the systems.
- C2: Poor support of human factors and design of meaningful human control, due to a strong technology focus and missing holistic focus on support of safety critical tasks across a distributed organisation.
- C3: Ground breaking automation has been successful based on user centered design, but in general there is poor research-based systemization of reasons for successful implementation of automation.
- C4: The offshore user environment is often so complex and based on missing HF considerations that there is poor compliance and understanding of risks in operations. Poor compliance and risk awareness are often used as causes in accident investigations, without going deeper to understand why.
- C5: Accident investigations seldom analyzes human factor issues and poor design of systems, leading to poor feedback and learning – continuing with more of the same technology focus, ignoring HF.

A key objective of MAS is to build knowledge of how V&V guidelines can address the issues C1 and C2 in an efficiant and cost reducing manner. To prioritize guidelines based on accidents and successes, another key objective of MAS is to systematize successful experience and improved safety from industrial automation, as identified in C3. To improve learning, and feedback to design, the issues C4 and C5 must be addressed. To ensure that best safety practices are employed by the industry during digitalization and design, a key objective is to implement and improve guidelines and methods that has consensus in the industry, such as the CRIOP method, addressing these challenges.

Automation and control systems relieve people of tasks, but automation challenges sensemaking and requires more, not less interaction design, interface design, and attention to training (Parasuraman & Riley, 1997). Failures in highly automated systems may be difficult to discover and to solve, and the term “out-of-the-loop” (OOTL) has been coined to refer to performance problems (Endsley & Kaber, 1999). When tasks are further automated in more complex settings, the operators’ roles and possibility to interact with the system change, often in unanticipated ways (Dekker & Woods, 1999). There is a need to gather more knowledge from OOTL incidents and recoveries when automation and remote operations are implemented in the petroleum industry. Numerous examples of poor implementation of meaningful human control in automated systems and remote control exists, such as the Deepwater Horizon Accident (CSB, 2016), Gas Well Blowout and Fire at Pryor Trust Well 1H-9 (CSB, 2019), the Boeing Max 737 accidents (Endsley, 2019), and the Helge Ingstad collision (AIBN, 2019). These point out the need for human factors participation and use of human factors standards, especially for assessment of safety critical tasks. Designing to get several cues in critical operations are ways to ensure redundancy in the system. Redundancy can provide the ability to recover to the needs of a dynamic environment (Hollnagel & Woods, 2005). Design decision, such as reducing complexity through operational domain design (SAE, 2018), and exploring strategies for resilience to cope with the unexpected (Hollnagel 2015), will increase the possibility of safe operations. The use of resilience engineering in automation is a relevant approach to handle unexpected events. Thus we are planning to collaborate with the industry and NTNU department of design to test and evaluate different strategies/solutions for resilience in design of control facilities as the project evolves. Concepts such as augumented teaming, Lützhöft (2019) will be explored. We see the need to learn from successful automation in other industries and build more knowledge on how sensemaking (as explored in Kilskar et. al 2020; AIBN, 2019) is supported in safety critical tasks. This will enable meaningful human control in automation and remote operations and continue to sustain word leading HSE in operations. Thus, it is an objective of the project to collect best practices and learning points from other industries when new technology is implemented. Automation in road transport is developing rapidly. TU Delft has gained relevant knowledge through their project “Meaningful Human Control over Automated Driving”, and they are involved in the project. The experience from other industries, such as aviation, show that pilots are able to compensate for automation deficiencies in unanticipated situations and that systems can support the operators in diagnosing and decision making. For example, Fiorino (2008) describes that developments have reduced the rate of fatalities to 0.01 per 1 million flight hours in aviation. Automation in aviation has

been supported by extensive focus on Human Factors, as an example through function flexibility and overlap between human and automation in joint cognitive systems supporting meaningful human control.

The selection of the CRIOP method is based on its successful use in the oil and gas industry since 2003. CRIOP is a HF guideline and a verification and validation tool to be used during design and operation of control systems, facilities or control rooms. The method is used internationally, also in shipping and has been adapted to be used in Space Operations (by ESA). The method is used daily in the Norwegian oil and gas industry and has been a state-of-the-art method. Use is based on a learning arena, a verification part with best practices and a validation through scenario analysis. There is a need to adapt and advance the CRIOP methodology to the increasing implementation of new automated technology such as AI. This is necessary in response to regulatory reform and evolution of technical codes and standards, to support emerging operational trends, and to be able to support meaningful human control

Analysing the risks of automation and complex systems are demanding. We have seen that Failure Mode, Effects & Criticality Analysis (FMECAs) and similar approaches are not well suited to cover complex systems with dependencies. Automation and remote operations lead to challenges with control, and there is a need to adapt new methods and approaches. A promising candidate is the System Theoretic Accident Model and Processes (STAMP) (Leveson, 2012). The most well-developed STAMP-related tool is the Systems-Theoretic Process Analysis (STPA) method, which can be used to identify multi-level safety constraints required to control safety in sociotechnical systems (Leveson & Thomas, 2018). CRIOP has been using the simplistic STEP model (Sequentially Timed Event Plotting) from Hendrick, and Brenner (1987) to explore scenarios. STEP is an excellent tool for user communication and exploration of well-defined scenarios; however, we see a need to explore a more holistic method when automation and remote operations are being used, and complexity increases. It is therefore an aim of the project to explore whether STPA can provide additional value and compliment the STEP method when analysing certain digitalized systems.

## 1.2 Research questions and hypotheses, theoretical approach and methodology

Table 1 gives an overview of the study's research questions and the tasks that have been designed to answer these questions. (In addition, we have two tasks of dissemination and project management, described in Table 2). The scope will focus on oil and gas but include cases from automation/remote operations in aviation, automated car/buses, metro systems and shipping. Answering these research questions will build knowledge to be used for risk-based guidelines for digitalization, to promote learning from success in other industries and update validation and verification methods for meaningful human control. The suggested research methods include literature reviews, industry interviews, exploration of cases, workshops, validation and improvement based on simulations and pilot testing.

| | | |
|---|---|---|
| **Aim** The aim of the project is to increase safety, efficiency, and productivity in critical operations, with meaningful human control when needed. | | |
| **Key objectives are** to build knowledge of how to design and operate control systems to avoid accidents in automation and remote operations; how to utilize successful automation and remote operations in design; and how to build on this knowledge in guidelines and methods that are used in the industry. | | |
| **RQ** | **Research Question** | **Task** |
| **RQ1** | What are the main safety challenges in design when implementing increased level of digitalization? | **WP1:** Learning from accidents and incidents in automated and remote operated systems. (To improve practices).<br>**WP2:** Review of safety challenges and practices in design of safety critical control systems – automation/remote operations. Focusing on sensemaking and meaningful human control of automation and remote operations. (To improve practices) |
| **RQ2** | What are the main reasons for successful digitalization? | **WP3:** Review of successful design, implementation and operation of automation and remote control, including successful recoveries. Explore suggestions in simulations. |
| **RQ3** | What are the main design guidelines for meaningful human control and resilience engineering in digitalization, and what are best practices to be used in the verification and validation method CRIOP? | **WP4:** Compile and analyse current practices, systematisation and structuring of design standards, guidelines and regulation related to automation, and remote operations.<br>**WP4b**: Develop methodology to include sensemaking in safety critical task analysis<br>**WP5:** Assess practice in use of CRIOP and improve the CRIOP method. Share relevant practices with the Canadian project – CRIOP-DO.<br>**WP6:** Validate and improve the methods through use in relevant areas in Norway and Canada to broaden experiences. |

**Table 1 Research questions and tasks**

### 1.2.1 Research approach

Safety critical systems needs to be designed based on knowledge from research and experts from a wide variety of disciplines including human factors engineering, industrial/ organisational psychology, management science, sociology, anthropology and information science. In this project, a multidisciplinary approach will be ensured through project participants from these disciplines and through the use of participatory action research (PAR), involving these stakeholders. The research is based on a risk-informed approach in combination with learning from successes and exploration of design guidelines supporting meaningful human control. To ensure cross industrial learning we have focused on cases – oil and gas industry as the primary focus; but also learn from aviation (autonomy and drones), autonomy in car/bus-operations, rail/metro transportation, and maritime sector (unified bridge concepts and autonomous systems). In the following we have described the theoretical approach and methodology which will be used to answer each of the research questions, methods and tasks for each WP are described in Table 2.

**RQ1: What are the main safety challenges in design when implementing increased level of digitalization (automation and remote operations)?** Accidents give ample opportunities for learning when developing new technology for automated systems and remote-control facilities. Learning from the mentioned accidents and transferring relevant learning points is important to ensure safe development. Thus, the first task is to perform a systematic review of literature (trough work package WP1) and discuss the findings in a workshop. As automation modifies the role of the operator from active controller to a supervisor to monitor and assume control during failures, the design of interfaces becomes more important. This creates a need for guidelines for interfaces based on human abilities, especially in complex situations with interaction with several other systems. This will be the basis for WP2, performing a review of safety challenges in design of critical control systems and what processes and standards are needed. Different development processes are being used based on user participation, Lee et al (2017) (i.e. ISO 11064 and ISO 9241), design-based standards, and methods for agile safe development such as SafeScrum (Hanssen et al., 2018). Agile development is based on iterations and rapid feedback and has succeeded in speeding up development. But there is a need to integrate user centric principles with safety and the agile methods to ensure that key principles are followed during automation and remote operations, i.e. the design is based upon an explicit understanding of users, tasks and environments; user-involvement throughout design and development; an iterative process and inclusion of multidisciplinary skills and perspectives especially HSE knowledge and awareness. The results are going to be integrated in guidelines developed in WP5 and WP6.

**RQ2: What are the main reasons for successful digitalization (automation and remote operations)?** Traditionally safety research and safety management in companies have focused on learning from negative events, and how to avoid these. However, in recent years, another approach towards safety has emerged, which aims at also focusing on the successful aspects of operation, and how these aspects may be enhanced as a means to increase safety. Hollnagel (2015) names this approach Safety-II, related to the resilient properties of systems, i.e. how the system is capable of handling future adverse events. Through WP3, the project will explore the successful implementation of automated systems and remote control in other industries and how the lessons from these industries should be transferred during implementation of new technology. Suggested resilient factors are going to be explored and tested in a lab environment, exploring effects. We suggest synthesizing and learning from successes in oil and gas (remote operation experiences), and from high safety domains such as aviation, since the aviation industry shows unprecedented safety statistics with aviation accidents having declined over the last few decades (IATA, 2015). The results from WP3 will give knowledge into how resilience factors such as redundancy, controlled degradation, flexibility/diversity, manage margins close to boundaries, supporting common mental models and reduction of complexity should be integrated in guidelines developed in WP5 and WP6.

**RQ3: What are the main design guidelines for meaningful human control and resilience engineering in digitalization, and what are best practices to be used in the verification and validation method CRIOP?** There is a need to update, adapt and advance the CRIOP methodology which is used to verify and validate design of control rooms and facilities, both nationally and internationally, to the increasing implementation

of new automated technology. This is necessary to remain effective in response to regulatory reform and evolution of technical codes and standards, and to support current and emerging operational trends, including continuous implementation of new technology, such as increased automation and AI (Artificial Intelligence), robotics, drones, digital twins and completely new operational philosophies (e.g. remote operations of unmanned installations, and remote operation of several units in one control room).
This key issue of WP4 will be, based on the knowledge acquired in the previous work packages, to consolidate the CRIOP methodology with these emergent issues. An issue in the CRIOP methodology is interaction design and high-performance Human Machine Interface (HMI), which becomes increasingly important as automation and new philosophies are implemented. The HMI design must be based on a thorough task analysis (especially of safety critical tasks) and driven by a user-centric (agile) design. The tasks and the criticality dictate the information requirements, and how sensemaking can be built between the involved actors (on site, remote and supported by experts). The HMI design must be guided by a performance philosophy and efficient style guide ensuring proper use of colours/content, layout, hierarchy/navigation, alarm support and the ability of the operator to be supported by several systems/sources/cues to ensure a high level of situational awareness and sensemaking, see Hollifield, Nimmo et al. (2008). There is a need to develop methods to support sensemaking in safety critical tasks through high performance HMI and the task WP4b will handle this.
The Scenario analysis of CRIOP need to be improved to analyse, understand and control increasingly complex sociotechnical systems. In this project, we will adapt the Systems-Theoretic Process Analysis (STPA) method to scenario analysis of safety critical tasks and in analysis of selected automation projects in Norway, to identify a set of common safety requirements at the authority, manufacturer and user levels to be included in the model. In WP5 we will compare the identified safety requirements with existing and developing regulations in order to identify gaps and make recommendations to improve best practices.

**Development based on user participation through Participatory action research:**
The project will employ the ideals of participatory action research (PAR). PAR is a research approach that revokes the conventional division between researchers and research objects (Greenwood and Levin, 1998). PAR aims at creating a joint learning and reflection process between researchers and the various stakeholders holding interests in the problem under study. It involves three basic elements – research, action and participation. As an approach based on dialogue and involvement, it is well suited to address risks that are characterized by uncertainty and ambiguity (Renn, 2009). The project's empirical data will be gathered by means of semi-structured interviews of cases, in combination with step-wise implementation and exploration of new ideas/issues in the suggested metods during the project timeline. The interviews will be structured around a set of questions derived from the literature study and risk/vulnerability assessments. In addition we will explore design issues through simulations in a test establishment at NTNU Design. We will interview regulatory bodies with regards to their strategies both in terms of rule development and supervision. The information from the interviews will be used in a series of workshops structured as so-called search conferences discussing new methods and tools/issues. Search conferences is particularly suitable for unstructured problems where several actors are involved in both problems and solutions. (Levin & Klev, 2002). The participants will include a variety of stakeholders which will ensure the requisite variety (Westrum, 1993) that is necessary to challenge existing views on threats and methods for a more agile approach for development of rules and regulation. The project plans to collaborate with a parallel project in Canada. This collaborative setting will provide a roadmap for a new wave of collaborative, multidisciplinary research on risk, safety and human factors within major industrial operations undergoing digital transformation.

### 1.2.2 Possible risks that might endanger achieving the objectives:

We have identified three main risks of this project together with mitigating actions.
One is too much focus on technology and too little focus on human and organisational issues in the technology driven environment in the industry. The project has been staffed with researchers having a broad socio-technical background to ensure that human and organisational factors are equally in focus and will be presented to safety authorities, industry and consultants.

Another issue is the challenge of getting the industry to adapt to new standards and way of working. We have focused on broad user participation and collaboration from industry and the key consultants in the area, in order to ensure ownership. There is a strong positive agreement to participate and be involved. The last issue is the cultural adversity of engineering to embrace HF in combination with missing knowledge and competence on the science of human factors in the Norwegian industry. This has been planned to be mitigated by collaboration and more focus from the safety authorities, industry actors, workshops and focus among the HFC network in Norway. We have also planned to focus on HF teaching among engineers, at universities (and colleges) and international collaboration to share HF training and best HF practices.

### 1.3 Novelty and ambition

Despite there being a rich set of data from the petroleum industry that can give us insights both in challenges and successes, there is a lack of sharing of experiences from incidents and challenges related to increased automation. The poor availability of published research in scientific journals discussing successes of automation in an MTO perspective will be addressed in this project through establishing a scientific foundation to understand the successes of automation. New knowledge is expected related to

- Meaningful Human Control of autonomous systems in development and implementation of new technology in the petroleum industry (a significant challenge due to poor prioritazion of HF)
- Sensemaking as an operational concept including organisational, technical and human factors
- Adaptation of STAMP/STPA for use in the oil and gas industry to explore scenarios and incidents
- Remote operations of oil fields based on experience – building resilience and safety
- Sharing of best practices of regulation to other countries, such as of functional based regulation
- Updated CRIOP methodology mitigating contemporary industry challenges and supporting HF

Based on the proposed collaboration between regulators, industry, consultants and academia new knowledge and new methods will be used due to the PAR approach supporting local ownership and engagement. Establishment of an accepted CRIOP method used daily, will substantially help us to support this new knowledge.

## 2. Impact

The impact of the project is on several levels for improved safety and resilience of operations where automation and remote operations are implemented. The implementation of automation and digitalization have a strong focus on technology, with somewhat missing analysis of safety critical issues involving HF, and missing systematic strategies for design of meaningful human control. Thus, the ambition of the project is to adapt and sustain best practices in HF for an more agile development and use of resilience engineering to ensure that automation is supported by the users and can be trusted through use of meaningful human control. Results will be shared and used internationally, trough collaboration with Canada and TU Delft.

### 2.1 Potential impact of the proposed research

By improving the internationally recognised CRIOP method with the results of our project, we will have immediate impact on practices used in the industry and continue our role as having a world leading methodology for verification and validation. The outcome of this project is expected to provide huge benefits to both the quality and efficiency of technology qualification processes in terms of more suitable methodologies (i.e. STPA) for identification of potential human-automation risks in complex systems and a better tool (updated CRIOP) to be used for verification and validation (with more focus on issues such as automation, remote operations, HMI, and new areas). The use of new verification tools to prove compliance with safety requirements will also support harmonization of safety documentation. The ambition is to significantly reduce the cost and increase the speed of implementation, in addition to supporting methods that supports the “right” solution more rapid, enabling Norwegian Industry to be world leading in safe automation and remote operations. Several cases are going to be explored, such as successful remote operations of oil and gas-fields (cases from Total EP/Equinor, GDF Suez Aker BP), remote operations of a fully automated ferry in Trondheim (AutoFerry), experiences of meaningful human Control from TU Delft, experiences of Unified Bridge solutions on ships giving collected status of many sub-systems, remote operation of automated metro, increased remote operation of rail/metro based on ERTMS.

Through improved knowledge based on research from other industries, interviews and cases from the petroleum industry, focusing both on learning from failures and successes, a coherent set of standards to support agile automation based on human centred design will enable safe and timely implementation of digitalization. This, in time, will support also the competitiveness of other sectors in the Norwegian Industry. An updated CRIOP could provide great benefit to work performed within Technology Qualification (ref. DNVGL-RP-A203) and also approval work for autonomous vessels. In the safety conscious railway industry, large resources are spent in verification, validation, and approval of safety critical systems and railway control and command systems (CCS) for high-speed and conventional rail. The main challenge is a comprehensive set of rules and specifications that applies to prove compliance. With increasing digitalization (automation and remote operations) built into systems, regulation is demanding with respect to consistency and amount of requirements. An updated CRIOP-method will facilitate effective verification and validation of Traffic Management Systems (TMS), which constitute the control facilities in the new European Rail Traffic Management System (ERTMS). The design guidelines for meaningful human control and resilience engineering in automation including world leading validation and verification methods, will be relevant for organizing and structuring safety critical tasks in distributed organisations. By applying the guidelines sensemaking and resilience engineering perspectives will be systematically integrated as part of automation design to handle the unexpected.The project supports the UN sustainable development goals (SDGs) GOAL 8: Decent Work and Economic Growth; GOAL 9: Industry, Innovation and Infrastructure due to our focus on automation of dull, dangerous and dirty operations; and our support on safe implementation of innovative new technology.

### 2.2 Measures for communication and exploitation

The project has an extensive plan for open communication, as described in the WP´s (summarized in WP7) and plan for exploitation of the results. The results will be a result of participation between industry, the project team, collaborative network in Canada and the HFC forum, thus building a solid foundation for acceptance of the use of results from the project.
All results will be OA – Open Access. The project will publish four peer reviewed papers, an OA-book with ten chapters (on journal level) to support methodologies, and two reports describing methods. In addition, the different themes from the project will be presented in the HFC forum through experts and scholars.

## 3. Implementation

In this chapter we have described the organisation and management, the project team and the task allocation. The project is organized through a steering reference group from the industry, a core project team of experienced researchers from SINTEF, NTNU, TU Delft and TØI To be aligned with the industry, we have organized set of practitioners/users of methodology to give advice and the HFC knowledge network to be used in workshops and project activities. Collaboration with Canada is coordinated through joint workshops.
Table 2 gives an overview of the main activities, the cost and the responsible party (resp) .

| WP | Main activities, objectives and deliverables | Cost |
|---|---|---|
| 1 | **Learning from accidents and incidents in automated and remote operated systems**.<br>Objectives: Establish knowledge repository of scientific papers and reports of automated and remote operations with key learning points from accidents, especially related to design.<br>Method: Systematic literature review in scientific databases, discussion of findings in workgroups. Cross industry learning between oil&gas; automation in aviation/ Metro&Rail/ Road Transport<br>Description: Exploration of databases such as Scopus, ScienceDirect, SpringerLink, using key-words such as "human factors", "offshore", “remote "situational awareness/ sensemaking" "cognitive", "meaningful human control", "oil and gas", "autonomy", "automated", "user centred design", “design”… Use of Google Scholar to identify themes of interest. «Snowballing» based on key reports such as The Offshore Energy Safety Institute (OESI) "Human Factors and Ergonomics in Offshore Drilling and Production: The Implications for Drilling Safety".<br>Results: Journal paper of key issues from incidents in automated and remotely operated systems - and repository of relevant papers as a part of a knowledge web. | 1,500<br><br>Resp: SINTEF |
| 2 | **Review of safety challenges and practices of design of safety critical control systems (automation/remote op.)**<br>Objectives: Identify safety challenges in design, identify existing and emerging practices in use and best practices across the relevant industries that can be shared and be used in learning lessons | 1,000 |

| | | |
|---|---|---|
| | Methods: Review of relevant new technology issues, Review of standards as suggested by standardization groups and regulators in the US, UK, Canada and Norway, Interview of experts involved in design cases from oil&gas, cars, rail, aviation and shipping. Workshop with industry.<br>Description: Document relevant new technology challenges (such as AI use and how to understand AI choices, and standards such as ISO/IEC TR 5469), Review safety challenges in design, Review design practices of safety critical systems. Gather best practices from innovation-based design (Design Council), agile design where safety is of key interest (such as SafeScrum), and design based on user centric development (such as ISO 11064), and sequential development (VEE-methods). Identify best practices in design of complex systems used to manage safety critical operations, and key issues that should be handled during verification and validation to ensure safety and resilience. Exploration of needs for high performance human interfaces (HMI) in different levels of automation (LOA).<br>Results: Journal paper with suggestions for best practices of design of safety critical systems and a repository of relevant papers and standards as a part of a knowledge web. | Resp: SINTEF |
| **3** | **Review of successful design, implementation and operation of automation and remote control, including successful recoveries.**<br>Objectives: Document key learning points that can be shared of successful remote control and high safety and resilient automation.<br>Methods: Review of relevant scientific papers. Exploration of cases through interviews (Remote operations in oil&gas Total-EP and Ivar Aasen; Remote operation of automated buses, and Metro in Copenhagen; Automation of Industrial transport; Automation of cockpit operations in aviation.) Workshop to discuss experiences across industrial sectors. Explore resilience in design through lab testing at NTNU Design, to explore consequences of resilience in design.<br>Description: Review of successful automation areas and successful remote operations of safety critical processes. Two different reviews – one focusing on safety and resilience of automation; one focusing on safety and benefits of remote operations. Focus will be on operational design i.e. scope, development process used, level of user participation, how knowledge sharing is performed, how learning and improvement has been performed based on incidents, how trust has been developed.<br>Results: Two Journal articles, one documenting key elements of successful practices of automation (and resilience) and one documenting experiences of remote operations | 1,500<br>Resp: NTNU |
| 4 | **Compile and analyse current practices, systematization and structuring of design standards, guidelines and regulation related to automation, and remote operations.**<br>Objectives: Suggest guidelines and regulatory practices that has user support based on coordination of findings from work packages<br>Methods: Document analysis of current practices and industry interviews, workshops with experts from different areas to select methods that has support from industry, experts, users and regulators.<br>Description: Coordinate findings from incidents, successful operations and design practices. Identify areas that needs integration of several methods and techniques. Identify current practices, existing gaps, identify barriers to implementation, identify guidelines and regulatory practices that has user support that should be a part of standards and methods. Identify training needs and structure.<br>Results: Open Access book with ten chapters describing findings from WP1..3 and needed mitigation, describing suggested design standards, guidelines and regulatory practices (see WP 7 for more details) | 1,500<br>Resp: NTNU |
| 4b | **Develop methodology to include sensemaking in safety critical task analysis**<br>Objectives: Describe how sensemaking can be supported by safety critical task analysis, and how high-performance HMI can be utilized to support sensemaking.<br>Methods: Development of methods based on review of practice and results from WP1..3.<br>Descriptions: Review of articles describing sensemaking in critical operations, and review of safety critical task analysis; building approaches to combine sensemaking and safety critical task analysis based on levels of automation. Use methodology on selected cases to check usability and validity.<br>Results: Methodology describing sensemaking in safety critical task analysis | 1,000<br>Resp: SINTEF |
| 5 | **Assess practice in use of CRIOP, and improve the CRIOP method**<br>Objectives: Improve existing version of CRIOP based on experiences from industry, changes in regulation, standards, practice and new technology prioritised by the industry.<br>Methods: Industry interviews, review of CRIOP reports, systematic work with industry reference group (i.e. discussion of scope, identify prioritised changes, follow up and evaluate and test new versions, implement new versions), focused workshops with industry and human factors experts; collaboration with Canada (with a prescriptive regulatory practice moving to a more performance-based regime).<br>Description: CRIOP continues to be commonly applied, however there is a recognised need to update, adapt and advance the methodology to remain effective in response to regulatory reform and evolution of technical codes and standards, and to support current and emerging operational trends, including: Digitalization (automation and increased remote operations); Automation with little human interactions and integration of AI (Artificial Intelligence) and the need to understand process states that require human intervention; Introduction of new technologies such as robotics, drones, digital twins; Completely new operational philosophies (e.g. remote operations of unmanned installations, and remote operation of several units in one control room); and continuous focus on risk and performance-based regulation supported by verification and validation. Finally, to specify and realise adequate assessment procedures supporting the updated CRIOP-method in collaboration with the CRIOP-DO project. | 1,500<br>Resp: SINTEF |

| | | |
|---|---|---|
| | Results: Updated CRIOP method (i.e. restructured checklists, more focus on conditions to perform a CRIOP analysis), extended scenario analysis, improved focus on integration of design processes, user-based design, and agile development supporting safety (SafeScrum). | |
| 6 | **Validate and improve the suggested methods through use in relevant areas**<br>Objectives: To validate the proposed method to support sensemaking and the proposed CRIOP amendments. The method will be assessed for their theoretical validation and practical applications.<br>Methods: The application of the proposed methods will be tested in two steps. Step 1 is to employ the proposed standard to a simulated and relevant industry scenario. It will be based on prior project experience. Step 2 advances the validation by integrating the methods in commercial projects (in full transparency with all stakeholders). The theoretical foundation is based on the generated knowledge from WP 1-3, but will be structurally assessed (e.g., workshops, interviews and review sessions) by third parties (I.e., personnel not involved in WP 1-3) in the current WP 6. Finally, open discussion with peer subject-matter-experts.<br>Description: The purpose of the current WP is to investigate the validity of the proposed methods. The focus is on the theoretical validity and on the practical applicability of the methods. The scientific connection, i.e., its theoretical underpinnings, are of paramount importance to have industry consensus and trust in the proposed methods. Thus, the current WP aims to provide the users of the standards with a transparent and well-document representation of how the standards are connected to state-of-the-art theory (provided in WP1-3) and robust testing (achieved through simulation and real-life application). Finally, the results from this WP will be subject to open discussion by key stakeholders within the HFC meeting. Projected scope of testing: Land based control centres coordinating several assets, Control rooms supporting drilling operations remotely, Control rooms for automated maritime operations, pilot testing – highly automated such as the AutoFerry in Norway).<br>Results: Experience report – used to improve the method. | 1,500<br>Resp: SINTEF |
| 7 | **Dissemination – articles, book and web of knowledge (Part of task 1-6)- Resp:SINTEF**<br>Objectives: Publish and disseminate results from the project through reports, methods and publications of peer reviewed papers, conferences, and 10 presentations and discussions at the HFC meeting. Disseminate publications as open access through web of knowledge.<br>Methods: Open Access publication and web-publication of papers, reports and book<br>Description of OA Book: Ten articles giving background for methods, based on WP´s. Describing safety challenges, best practices in design, best practices of automation and remote operations, agile user Centered processes, suggested analyses techniques, essential guidelines in automation, conducting workshops exploring safety cases, experiences from verification and validation.<br>Results: Four peer reviewed articles (from WP1, WP2 & WP3), Updated CRIOP method, OA book. | |
| 8 | **Project management** Objectives: To manage the project within financial boundaries and produce results as described. Methods: Result oriented project management, with two formal status reports each year based on expected results that should be produced. | 500<br>Resp: SINTEF |
| | **TOTAL Budget** | **10,000** |

**Table 2. Activities, costs and responsible parties.**

Budget is to be covered by contributions from the HFC forum (in accordance with existing EU/EØS rules and regulation) and from the Research Council.

## 3.1 Project organisation and management

The project will establish a steering reference group, a core project team (with support from a local expert group), user network (via a user practice team and the HFC collaboration network). The project will collaborate with the CRIOP-DO project in Canada.

**The steering reference group** consists of the oil and gas companies Aker BP, Equinor, Vår Energi, Sintef (agreement to participate). Meeting frequency (minimum each year) related to the WPs and key issues to be discussed, adjusted as needed.

**The project team** will consist of a core team and a user practice team that want to participate in the development of new methods. The core team will consist of researchers from SINTEF, NTNU, TU Delft, TØI with a multidisciplinary background.

**The user practice team** will consist of users involved in actual project work and that will perform review and testing of selected parts of the methodology.

**The user community** will be represented by the HFC network, that will participate in workshops and conferences to discuss and comment on methods and practices.

## 3.2 Project manager and project group

The project will be managed by SINTEF from the Safety research group at SINTEF Digital. The research team is multidisciplinary, consisting of researchers from both engineering science and social science. The team have relevant experience and publications in the areas essential to the proposal. The participant consists of SINTEF, the Norwegian University of Science and Technology (NTNU), TU-Delft and TØI.

NTNU Design will finance 50% of a 3 year Post Doc as a part of the project.

## References


Aas, A. L., Johnsen, S. O., & Skramstad, T. (2009). CRIOP: a human factors verification and validation methodology that works in an industrial setting. Esrel (pp. 243-256). Springer, Berlin, Heidelberg.

AIBN (2019) - Part one report on the collision on 8 November 2018 between the frigate HNOMS Helge Ingstad and the oil tanker Sola TS outside the Sture terminal in the Hjeltefjord in Hordaland county.

BRU21 (2020) BRU annual report, retrieved from https://www.ntnu.edu

CSB (2016) U.S Chemical Safety and Hazard Investigation Board. Drilling rig explosion and fire at the Macondo well. Investigation report volume 3, Report no. 2010-10-I-OS, Washington, DC: U.S Chemical Safety and Hazard Investigation Board.

CSB (2019) U.S Chemical Safety and Hazard Investigation Board, Gas Well Blowout and Fire at Pryor Trust Well 1H-9 Washington,

Dekker, S. and Woods, D. D. (1999). Automation and its Impact on Human Cognition. In S.Dekker and E. Hollnagel (Eds.), Coping with Computers in the Cockpit (pp. 7-27).Aldershot, UK: Ashgate.

Endsley, M.R. & Kaber, D.B. (1999). Level of automation effects on performance, situation awareness and workload in a dynamic control task, Ergonomics, vol. 42, 462-492

Endsley, M., (2019). Human Factors & Aviation Safety, Testimony to the US House, Hearing on Boeing 737-Max8-crashes.

Fiorino, F. (2008). New benefits, new risks. Aviation Week and Space Technology (New York) 169(14): 49-51

Greenwood, D. J., & Levin, M. (1998). Introduction to action research: social research for social change. Sage

Hanssen, G. K., Stålhane, T., & Myklebust, T. (2018). SafeScrum -Agile Development of Safety-Critical Software. Springer International Publishing. K., Brenner, L., 1987. "Investigating Accidents with STEP" Marcel Dekker, New York.

Hoem et al. (2020) "Improving safety by learning from automation in transport systems with a focus on sensemaking and meaningful human control." in Taylor &Francis- Sensemaking in Safety Critical Situations:, Ed: Porathe& Johnsen, in print

Hollifield, B., Habibi, E., Nimmo, I., & Oliver, D. (2008). The high performance HMI handbook: A comprehensive guide to designing, implementing and maintaining effective HMIs for industrial plant operations. Plant Automation Services.

Hollnagel, E. & Woods, D. D. (2005). Joint cognitive systems: Foundations of cognitive systems engineering. Taylor & Francis

Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). From Safety-I to Safety-II: a white paper. The resilient health care net

Hagenzieker, M. (2020) Meaningful Human Control newsletter MAY 2020 #5, TU Delft

IATA. (2015). Loss of Control In-Flight Accident Analysis Report, 2010-2014.

ISO series 11064:2000 – "Ergonomic design of control centres".at https://www.iso.org

ISO series 9241:2020 – "Ergonomics of human-system interaction" .. at https://www.iso.org and ISO/TR 9241-810 Ergonomics of human-system interaction — Part 810: Robotic, intelligent

Kilskar, S. S., Danielsen, B. E., & Johnsen, S. O. (2020). Sensemaking in Critical Situations and in Relation to Resilience—A Review. ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg, 6(1).

Lee, J. D., Wickens, C. D., Liu, Y., & Boyle, L. N. (2017). Designing for people: An introduction to human factors engineering.

Levin, M., Klev, R. (2002). Forandring som praksis: læring og utvikling i organisasjoner. Bergen: Fagbokforlaget.

Leveson N (2012) Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge

Leveson, N.G. & Thomas, J. (2018). STPA Handbook. Retrieved from https://psas.scripts.mit.edu

Lützhöft, M. H. (2019) Proceedings of Ergoship 2019. "Siri sail the ship".

Mecacci, G., & de Sio, F. S. (2019). Meaningful human control as reason-responsiveness: the case of dual-mode vehicles. Ethics and Information Technology, 1-13.

Ptil (2020) - Johnsen, S. O., Holen, S., Aalberg, A. L., Bjørkevoll, K. S., Evjemo, T. E, Johansen, G, Myklebust, T., Okstad, E., Pavlov, A. & Porathe, T. (2020). Automatisering og autonome systemer: Menneskesentrert design. SINTEF rapport 2020:01442.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39(2), 230-253.

Renn, O. (2009). White Paper on risk governance: Towards and integrative approach. IRGC.

SAE (2018). SAE International standard "J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems." Revised: 2018-06-15

Santoni de Sio, F., & Van den Hoven, J. (2018). Meaningful human control over autonomous systems: A philosophical account. Frontiers in Robotics and AI, 5, 15.

Westrum, R. (1993). Cultures with Requisite Imagination. In J. A. Wise, V. D. Hopkin & P. Stager (Eds.), Verification and Validation of Complex Systems. Berlin: Springer.