Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4161-cd

Meaningful human control in digitalization, automation/AI, and remote oversight

Stig O. Johnsen

SiPå, SINTEF, Norway. Stig.O.Johnsen@sintef.no

Jooyoung Park

Department of Design, Norwegian University of Science and Technology, Norway. jooyoung.park@ntnu.no

Meaningful human control (MHC) of safety critical systems is a important goal as digitalization, automation/artificial intelligence (AI), and remote oversight are implemented. In the EU/AI regulation, the concept of human oversight is introduced, especially for safety critical operations. MHC and human oversight are challenging because they depend on human strengths and weaknesses, system design, knowledge and training, and organizational factors like responsibilities, staffing, and work processes. MHC is more useful than human oversight because it ensures that systems, technology, and organizational structures are designed to keep humans in control of safety-critical operations, thereby preventing disasters. However, to be useful, MHC needs to be defined and specified. This paper aims to define MHC by addressing three key areas: design, operations, and learning. Key design issues for MHC include adopting a system approach, using human-centred design best practices, conducting task analysis to manage cognitive workload, creating consistent interfaces for quick situational understanding, designing alarms to support situational awareness (SA), and establishing work processes that promote shared SA across teams. Key operational issues include ensuring safety, managing change (MoC), addressing error traps and training, and maintaining physical and mental conditions to enable MHC in all situations. In a critical situation, we observe that it can take 10 minutes to observe, understand and act correctly in crises. Main issues in learning from accidents must be to identify root causes including poor concepts/design and trying to understand reasons for human SA and actions. We have used "Human Error" as a starting point for analysis. Learning and understanding should drive change and improvement in governing values, prioritizing learning over blame.

Keywords: Meaningful Human Control, Safety, Human Factors.

1. Introduction

The rapid adoption of digitalization, automation, and AI in industries such as oil and gas and transportation has transformed traditional workflows, enabling remote operations and reducing human workload. However, these advancements also introduce significant challenges, particularly in ensuring Meaningful Human Control (MHC) over safety-critical systems. MHC is essential to address the limitations of automation. Bradshaw (2013) debunks myths of full autonomy, and that autonomous systems eliminate human oversight. Bainbridge (1983) points out an irony: as automation increases, operators require more training for rare interventions. Hancock (2021) identifies a paradox: while supervising autonomous systems can be monotonous and reduce vigilance, crises require quick and skilled responses. These challenges highlight the need to assess the role of the human operator to ensure MHC. We must design based on realistic expectations for what the human operator can do, control work as done in operations, and learn to handle the rare and crucial events.

The National Institute for Occupational Safety and Health (NIOSH) Prevention through Design (PtD) initiative in the United States recognizes that designing out or minimizing hazards and risks early in the design process is one of the best ways to prevent occupational injuries, illnesses, and fatalities (Behm et al., 2014). Meaningful human control (MHC) has been used since 2010, discussing autonomous weapon systems and later being used in the discussion of autonomous car systems, Mecacci et al. (2024). Initially, MHC was applied to weapon systems, emphasizing that humans—not computers or algorithms—should control decisions affecting Health, Safety, Security, and Environment (HSSE) (Calvert et al., 2024). Operational issues are central to MHC, and human limitations must be addressed to achieve meaningful control. Humans must be able to understand and control situations effectively. The knowledge of human limitations and possibilities has been based on the science of Human Factors (HF), defined as "*the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and methods to design to optimize human well-being and overall system performance*." IEA (2000).
In this paper we have used MHC as a goal and operational principle that can be achieved through addressing three key areas: design, operations, and learning. The goal of MHC should be a widely supported principle. However, achieving it requires a system perspective that integrates humans, technology, and organizational factors (MTO).

We propose that MHC should be established and maintained through a continuous learning cycle, spanning design, operations, and feedback, i.e.:

- Design issues, including governing factors such as laws, regulation, and audits impacting the system; System scoping and problem definition; Use of methods and system design activities including safety critical task analysis – SCTA.
- System Operational conditions i.e.: workload, training, procedures, organization, and qualities such as SA "at a glance" from HMI - Human Machine Interface.
- Learning and improvement from accidents based on an investigation model avoiding shortcuts such as "Human Error". Prioritize the exploration of design issues, trying to avoid blame and change governing factors.

Our definition of meaningful human control is: *Meaningful human control is the ability of a system (with humans, technology and organization) to be controlled by humans to avoid accidents impacting HSSE, subject to human abilities and limitations (in the context of the science of HF).*
Human Oversight (EU/AI act) focuses on ensuring that high-risk AI systems are designed to allow persons to monitor and intervene in their operation to mitigate risks to health, safety, and fundamental rights.
MHC is an operational principle that ensures that humans remain decisively engaged and capable of intervention in automated systems, thus ensuring humans remain in control of safety-critical operations. MHC is dependent on design issues (scoping and HF knowledge), operational practices and the ability to learn and improve based on investigations and continuous learning. Based on the above context, the research questions we have selected are:

- RQ1: What design issues enables MHC?
- RQ2: What operational issues sustain/ensures MHC?
- RQ3: How can we learn and improve MHC from incidents?

2. Approach and Methods

Approach: This research adopts an action research (AR) approach Greenwood & Levin (2006), which emphasizes collaboration between researchers and stakeholders to address real-world problems and develop practical solutions. Through prolonged engagement, interviews, and workshops, we identified key lessons to define and operationalize MHC. The AR approach has proven effective in improving safety in various contexts Antonsen et al. (2007).

We define MHC using theories and practices from Human Factors (HF) and Safety Science. HF is the natural foundations of meaningful human control, and safety should be the result of MHC. Accidents reveal the quality of MHC, and investigations—incorporating HF perspectives—can identify ways to improve MHC approaches and methods. We have used the perspectives from the science of human factors (to help discuss design issues and operational conditions). We used the hierarchy of controls (Manuele, 2005) to prioritize our findings. We have used the understanding of accidents from methods used in accident investigations to learn and improve.

To address the research questions, we conducted a literature review, performed expert interviews, and case studies. The scope of the literature review was to explore relevant HF papers with lessons from accidents involving automation and remote operations. We have chosen to explore best practices of human control in safety critical environments such as flight cockpit, ship bridge, road traffic and process industries. We have included snowballing from relevant papers, building on results from Johnsen & Winge (2023). Empirical results of AI/automation and remote operation has also been explored and discussed such as in Park et al. (2025). An excellent survey of HF design practices from aviation is given in Kirwan (2025). These practices have established aviation and piloted flights as the safest way of transport; thus, they have been a source of best practices, Johnsen et al. (2024a).

Method from design through learning from accidents: The Hierarchy of Controls is a safety framework used to minimize or eliminate hazards. The American National Standards Institute (ANSI) states that the hierarchy of controls "provides a systematic way to determine the most effective method to reduce risk associated with a hazard" ANSI (2012, p. 15). A systematic empirical study (Dyreborg et al., 2022) supports the hierarchy of controls. It organizes safety interventions by their effectiveness, from the most effective (eliminating the hazard initially) to the least effective (relying on personal protective equipment/PPE). We have used the hierarchy of controls as defined by NIOSH (2024), and Manuele (2005), both to validate our approach starting with design, and as a prioritization guide. The issues in a prioritized manner are:

1. Elimination, of hazards and risks through definition or design, through scope/ problem reformulation/discussion, redesign, reorganization
2. Substitution, using other approaches i.e. automation, manual systems, other redundant systems
3. Engineering controls, through alarms, HMI to get status at a glance, workload assessments
4. Administrative controls, procedures, training
5. PPE- Protective equipment (barriers at the individual level)

The understanding of accidents is based on methods used by Norwegian Safety Investigation Authority NSIA (2022) and Australian Transport Safety Bureau ATSB (2007). They are referencing theories of organizational accidents Reason (1997) and how the involved individuals understood the situation, i.e. situational awareness, using Endsley & Jones (2012). The key steps in the accident analysis model are to explore from occurrence to identify causes, described by ATSB (2007):

1. Occurrence of events describing the incident
2. Local Control – aspects influencing the incident
3. Risk Control – barriers in place to reduce possibility
4. Organizational influences – responsibilities, MoC
5. Regulative oversight – auditing, laws

For learning we adapt the investigation methods, focusing on: 1)Event sequence & the SA of the actors involved as suggested by Safety forum (2019); 2) Local Control and Risk Control affecting MHC; 3)Design flaws rooted in poor problem definition, methods, regulation and organizational influences.

3. Results and discussion

Findings has been structured in three main areas based on the research questions i.e. key design issues; key operational issues; key issues to learn and improve. The findings have been based on literature reviews, exploration of accidents and discussion with experts in workshops.

3.1. *Key design issues*

The best ways to achieve safety are to build on regulations, use best practices from HF and 'design out' or minimize hazards and risks early through the design process. Effective design underpins MHC. We have tried to identify best practices by learning from the aviation industry having exceptional high safety, efficiency and usability. We have identified necessary steps to use new technology in a safe manner, identified how regulation can support best practice such as HF. We have

identified the need for a through system scoping, the benefits of using human-centred design and task analysis, the needed guidelines to design usable alarms, and the need for user testing.

Learning from best practice in Aviation: Aviation has such a low accident rate that they are characterized as ultra-safe Amalberti (2017). IATA -The International Air Transport Association managing 82 % of all air traffic had no hull losses in 2012 or 2017, supporting the view that aviation is a leader in safety. The aviation industry has initiated and integrated HF as a mean to support human control in their working environment from World War II, see Kirwan (2025). Key safety issues from aviation are the prioritization of HF and the open reporting culture prioritizing learning vs blame (i.e. Just Culture). Where "Just Culture" is a part of regulation, described as: "*A culture in which the front-line operators or others are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but where gross negligence, wilful violations, and destructive acts are not tolerated*" EU (376/2014) Aviation Safety. Practice from aviation has been transferred to other industries, such as the science of HF and just culture, and are a part of key design issues supporting MHC.

Maturity matters: Technology development must be adapted to the users. However, human factors are often an afterthought in the Oil and Gas industry. This is mentioned by Bergh et. al. (2024), pointing out that there is a lack of focus on human factors in both development projects and in operations. However, this can be mitigated using Human Readiness Level-HRL ANSI/HFES (2021), and Technology Readiness Level-TRL Yasseri et al. (2018). HRL and TRL are frameworks used to assess the maturity and readiness of technology in safety-critical systems. They play important roles in ensuring safety by evaluating how well technologies and human operators are prepared for real-world application, particularly in high-risk fields. By using HRL and TRL, organizations can proactively address both human and technological readiness, creating safer systems and environments. These readiness levels ensure that both the people operating systems and the systems themselves are sufficiently prepared, tested, and validated before deployment. This reduces the likelihood of accidents, improves safety performance, and ensures a safer working environment. Key benefits in using HRL and TRL are early identification of potential hazards, ensuring proactive risk management, Johnsen & Aminoff (2024). The framework help meet industry regulations, ensuring safety. The iterative assessments of HRL and TRL contribute to ongoing safety advancements. Well-prepared staff and technologies improve safety performance, reduce downtime, and prevents costly failures or accidents by ensuring readiness before full deployment. HRL optimizes interfaces to align with human capabilities, reducing probability of accidents. Moreover, HRL ensures workers are adequately trained, minimizing mistakes, and HRL readiness prepares workers to handle crises effectively. TRL ensures technologies are fully tested and safe before use (especially in combination with HRL), and confirms technology is reliable, ensuring safe operations. Use of AI in safety critical systems must follow the maturity development as described in HRL and TRL. Challenges with use of AI, NAS (2021), are **Brittleness (**AI will only be capable of performing well in situations that are covered by its programming or training data); **Perceptual limitations (**AI algorithms continue to struggle with reliable and accurate object recognition in "noisy" environments); **Hidden biases (**AI software may incorporate many hidden biases from being created using a limited set of training data); **No model of causation (**ML-based AI is based on simple pattern recognition; the underlying system has no causal mode. Because AI cannot use reason to understand cause and effect, it cannot predict future events). We have experienced challenges with poor sensor fusion and negligent neural network training and poor testing, see Cummings (2024). Use of HRL and TRL can mitigate this, and support MHC through human-centred design.

HF methods need support in regulation: In HSE (2015), they documented the positive promotors for using HF in the industry. They found that regulation mandating HF had a permanent effect on companies' willingness to consider human issues. Thus, prioritization of HF methods in regulation, such as ISO 11064 or ISO 9241-210 is a driving force for implementing HF practice. Regulation from the oil and gas safety authority in in Norway (the management regulations) mandates that ISO 11064 should be used (a standard based on HF experience). A more general standard is ISO 9241-210 highlighting principles of human centred design. Often used arguments against HF are the cost in the development phase, however the cost of poor safety leading to an accident can be significant as seen in the Deepwater Horizon disaster or the Boeing Max accidents. HF does benefit organizations through better compliance, reduced costs, and improved user trust. MHC is supported by HF methods, by their system/ MTO approach.

Scope smartly – Right problem & Right solution: Good practice highlights the importance of starting with a project definition/ clear scope including the MTO system, as described in Begnum (2021). The effect of an appropriate project definition is documented in Helgar (2022) and Bjørneseth (2021). Both demonstrated the benefit of a broad scoping looking at the whole MTO system, in combination with user centred development, utilizing task analysis. The result of design and implementation of the unified bridge concept, Bjørneseth (2021), was that they achieved high user satisfaction and was awarded safety and design awards. An important part of the project definition is tasks allocation between humans and technology (automation/AI), as discussed by "Fitts list", adapted by De Winter et al. (2014). The project definition and MTO scoping are an important enabler for MHC. However, the technology must be made mature, through development of the readiness level and user testing.

Human-centred design: The underlying principle of human-centred design is specified in ISO 9241-210 and is an important guideline when prioritizing meaningful human control. The standard aligns systems with real user needs, minimizing cognitive load. Early usability testing prevents costly mistakes and redesign efforts. Consistent design across interfaces improves learnability and adoption. Fewer user errors lead to lower operational risks and higher productivity. ISO 9241-210 ensures Human-centred design, improving safety, efficiency, and usability. **Safety** is enhanced through iterative testing, reducing human errors, and better regulatory compliance. **Efficiency** improves through optimized workflows, reduced training time, and fewer errors. **Usability** increases with

intuitive design, user satisfaction, and accessibility. Thus, implementing ISO 9241-210 results in safer, more efficient, and user-friendly systems. This was also a finding from Helgar (2022) and Bjørneseth (2021). However, a challenge when using ISO standards 9241-210 and 11064, is that the methods seldom identify practical techniques of Human Factors Engineering (HFE) to support the activities described in the methods, Leva et al. (2015). Examples of important techniques are task analysis, guidelines for HMI design (such as IEC 63303, based on ISA 101.01), alarm standards (such as EEMUA 191, IEC 62682), described in the following.

Task analysis. supporting MHC: SCTA is an important HFE technique to support MHC. As described by Energy Institute (2020), SCTA is used as a basis for designing HMI, procedures, and organizational responsibilities. SCTA structures and identifies user needs, ensuring decision-making support through HMI while reducing cognitive overload. By aligning interface design with task demands, it minimizes human errors and enhances usability. The standard IEC 63033 list good practice to improve HMI design, based on task analysis. SCTA ensures procedures are clear, structured around real-world workflows, and highlight potential failure points. This improves operational reliability and supports effective emergency response under high-stress conditions. SCTA defines clear roles and accountability for safety-critical tasks, improving teamwork and communication. It also enhances training programs, ensuring staffs are competent and well-prepared for critical operations. Bjørneseth (2021), used task analysis to understand "work as done" based on interviews, observation of work practices and exploration of personal adaptions. In addition, they used eye-tracking to understand user needs and used simulators and prototyping to develop usable concepts. Eye-tracking has also been studied in the oil and gas industry. It seems an effective tool to assess design and cognitive workload, and could lead to safety improvements, IOGP (2024). Task analysis helps determine what information is critical for operators to perform their tasks and to design the interface. By analysing tasks, designers can identify decision points, and the cognitive processes involved, ensuring the interface provides the right information at the right time. This is a starting point for Ecological Interface Design (EID). EID is a human-centred design approach that enhances decision-making in complex systems. This is done by providing visual representations of system constraints, relationships, and affordances. It aims to support both routine and unexpected situations by reducing cognitive load and improving situational awareness. The need for ecological interface design was highlighted in Meshkati (2006). An important issue was to match task demand analysis vs capability of the operator to handle difficult deviations (such as alarms).

Assess demanding workload and boredom: Many accidents have happened during high workload, such as when many alarms are sounding, or many different activities must be managed. The BP Texas City Refinery explosion in 2005 is an example of an accident due to high number of alarms and high workload. Often used method for assessing cognitive workload is NASA-TLX Stanton et al. (2017). To ensure MHC, workload and operational environment need to be assessed and managed, i.e. physical and cognitive workload based on task analysis (describing task requirements and a timeline analysis). Boredom and ability to handle surprises during low workload (defined situation of hazards) must be assessed and mitigated.

Alarm design and management: The design and management of alarms are critical in preventing industrial accidents. Especially in high-risk environments where the operator may be involved like chemical plants, refineries, oil and gas production, and transportation. Poorly designed or mismanaged alarm systems are a major factor in many accidents, as they can fail to provide timely or clear warning signals when hazardous conditions arise. Disasters due to poor alarm management are, among others, the King's Cross Fire in 1987 with 31 fatalities; the Piper Alpha Disaster in 1988 with 167 fatalities; the BP Texas City Refinery Explosion in 2005 with 15 fatalities and the BP Deepwater Horizon in 2010 with 11 fatalities. These incidents, HF issues, and best practice of standards are discussed in Briwa et al. (2022). They highlighted EEMUA 191 as one key standard with usable/ achievable guidelines. In the North Sea, there have been persistent alarm issues. The Norwegian regulator has published guidelines and performed audits, ref Bjerkebaek et al. (2004). They found that there were poor alarm handling and that the safety critical function of the alarms in a crisis situation may be impaired. Walker et al. (2014) conducted a review of 30% of North Sea control rooms, and found persistent issues around alarms, and poor support provided to operators in non-routine and emergency situations An alarm-audit was done in 2021-2022 by the Petroleum safety Authority in Norway, PSA (2022). Only one installation got no remarks. The same alarm-challenges can be found in shipping. Poor alarms and missing follow-on actions was found as key issues in the accident of Sjøborg- PSA (2019) and Viking Sky- Porathe (2023). In both cases, the systems issued several alarms, the alarms were not understood/ resolved, leading to more serious situations in this case by turning off power/ propulsion in safety critical situations. Effective alarm systems should be designed to alert operators quickly and accurately to potential dangers, allowing them to understand the situation and take appropriate action before situations escalate. Best practice standards, EEMUA 191 and IEC 62682 are suggested. EEMUA 191 has practical HFE guidelines, useful questionnaire, and relevant limits of number of alarms. However, alarms must be tested together with users.

User testing: Systematic user testing is also a key technique to improve usability, ensure MHC, and reduce costs, Norman (2013). User testing ensures that systems are intuitive, efficient, and meeting user needs. Conducting tests early helps identify and fix issues before they become costly problems. Early user testing identifies confusing elements and enhances user experience. It will reduce mistakes and supports clear workflows and intuitive interfaces. It will boost efficiency through streamlining of tasks, reducing effort and frustration. It lowers costs, through catching issues early and prevents expensive redesigns. It ensures compliance and aligns with industry standards like ISO 9241-210/ISO 11064.

In this section, we highlighted the need for using best practice, developing maturity through HRL/TRL, system scoping including MTO, build on user centred design/ISO 9241-210, use of Human Factors Engineering Techniques (SCTA, Alarm standards, workload), and prioritize user testing from the start.

3.2.*Key operational issues*

This section explores key issues related to operation such as maintaining responsibility in a chain of suppliers, night work, situational awareness and mitigation of error traps.

Maintaining safety responsibility in a chain of suppliers: Industrial actors are increasingly outsourcing and using suppliers/ contractors in their value chain, IOGP (2017). Safety issues in management of changes (MoC) is an important part of the management of contractors. IOGP (2017) recommends that the operator and contractor: "participate in site visits and challenge the performance of risk controls and barriers". This "see-to-responsibility" is defined in regulation and demands that operators and supervisors are actively involved in managing and overseeing safety. It ensures that risks are mitigated and that workers are properly trained and equipped to handle potential hazards. The Norwegian Ocean Industry Authority (Havtil) enforces regulations in the oil and gas industry, holding organizations accountable for maintaining a safe working environment. Description of the "see-to-responsibility" is found in maritime, i.e. Skipssikkerhetsloven (2007) and at Havtil (2025) i.e. the Petroleum Act, Regulation (Framework, Management), and Working Environment Act. As new technology and new ways of working are coming, the MoC can be challenging, and there may be a gradual shift to a more difficult/ demanding work environment. A challenging work environment of the outsourced driller was described by Equinor (2024), in the drilling conference in Kristiansand. Equinor highlighted the lack of holistic, human-oriented approach of cabin design and upgrades, distractions from core tasks, and inadequate workplace ergonomics. The operator has a "See-to" responsibility to ensure that the necessary actions to ensure workers' safety is done, supporting MHC.

Night work is risky: Many accidents or major disasters occur on night shifts due to changes in alertness due to circadian rhythm Smith (1994). Examples are Chernobyl, Three Mile Island and the Bhopal disaster, that have occurred at night between 24:00 and 05:00 Smith (1994). It is documented that night work increases the risk of accidents, Lie et al. (2014), thus night work requires good management planning to ensure MHC through eliminate/or reduce safety critical activities at nighttime or during change of responsibility (between shifts).

Sufficient time to establish SA: Loss of SA has been found as an important root cause in accidents. Sandhåland et al. (2015) analysed accidents of supply ships in the oil and gas industry, and mentioned that poor SA, (level 1), were causes in 13 of 23 accidents. The poor SA seems to be a result of poor interface design or insufficient training. Guidelines related to needed time to handle unexpected situations, is defined in alarm standards. EEMUA 191, specifies that six high priority alarms can be handled in an hour, i.e. 10 minutes are needed as a guideline for each alarm. From accident investigations we can discuss best practices, as the US Airways Flight 1549 (Airbus A320) that struck a flock of birds shortly after take-off losing all engine power; the pilots managed to glide the plane to ditching on the Hudson River, NTSB (2010). The pilots had long experience, excellent HMI/cockpit layout– they used 2 minutes to decide what to do, i.e. in our view an exceptional minimum time limit for decisions under duress. The automatic radar plotting aids used to avoid collisions at sea, are using between 1 and 3 minutes to identify problems. We cannot expect that the human operator uses shorter time in an unstructured environment. (Driving a car is more structured). SA is important to achieve but we must recognize the need for design, experience, training and sufficient time to acquire SA. If there is an accident due to poor SA in the system, we often have poor user design and too little time, and not a human failure. As Miranda (2019) notes - "Suggesting that an operator caused an accident by 'losing SA' indicates there are underlying design flaws within the system". SA must be designed, and we must explore poor design of SA as possible cause and not use "Human Error" as an easy excuse. To reformulate van Winsen and Dekker (2017) *we have an ethical and moral responsibility to defend the human operator who inherits a poorly designed system*, i.e. do not use SA to blame the operator. We must demand appropriate design to ensure MHC, i.e. that the flow of SA being supported by high performance HMI to get "situation at a glance" Hollifield et al. (2008).

Resolving error traps: Due to poor design, the system may have "error traps" that can create dangerous situations. Poor or missing MoC may also lead to drift into danger due to error traps. Often found error traps are poor equipment, stress, nigh time work, communication, poor staffing, unclear roles or responsibilities, outdated procedures, poor training or noise, Norsk Industri (2023). New error traps can also be introduced through AI, such as model drift that is not corrected, Cummings (2024). AI must be followed up in line with other systems. MHC is dependent on systematic reality check and MoC to avoid/ mitigate error traps. The reporting and follow up of error traps should be a key activity in high-risk conditions.

In this section, we highlighted the consistent responsibility across suppliers (i.e.: "See-to"), the need for follow up human limitations (late night work, necessary time to achieve SA, and error traps) and a systematic reality check of status.

3.3.*Key issues to support learning from incidents*

This section presents key issues related to MHC in relation to learning and improvement from incidents and accidents. The suggested sequence is: 1)Document events & exploring SA of the actors. 2) Local Control and Risk Control affecting MHC; 3) Design flaws rooted in poor problem definition, missing use of methods, and organizational influences.

Events and SA documented to identify MHC: A basic condition for learning, is to avoid blame. Systematic documentation should be established to foster understanding. We must start by understanding the sequence of events and the SA of the involved actors to document how the MTO system supported MHC during the incident. We are documenting the incident by a model easy to understand and communicate i.e. STEP the Sequential Timed Events Plotting diagram, Hendrick & Benner (1986). The STEP method is a structured, systematic approach that organizes events and involved actors chronologically to identify all actors and events as basis for root cause analysis. It provides a visual representation of the incident, integrates multiple actors/events, collaboration and support human factors, making it effective for understanding complex scenarios. In addition we try to document the SA of critical events, among the actors, using Endsley & Jones (2012) to document SA. This consists of: I.Perception– identifying critical elements in the environment (e.g., system status,

alarms, visual cues); II.Comprehension– understanding what the perceived information means in the current situation; III.Projection – predicting future system states and potential outcomes to make proactive decisions.

MHC from local control and risk control: Local control is based on the context or environment influencing individual actions or technical events, i.e. local error traps such as characteristics of individuals, physical environment, equipment, and tasks. These items are listed in CRIOP, Aas (2009). Conditions can increase safety risks through fatigue, poor ergonomics, insufficient knowledge, or high workload. Local conditions could influence technical issues, such as engine failures due to material defects or high operating temperatures. Risk controls are measures implemented by organizations to ensure safe performance, such as preventive controls (barriers). They aim to minimize the likelihood of undesirable events through design, procedures, responsibilities (including "see-to"), alarms, training or work rosters. Reactive or recovery controls (or barriers) detect and mitigate the effects of undesirable events, including warning systems, emergency equipment, and procedures. Defences-in-depth or lines of defence refer to multiple layers of risk controls that provide protection against system failures. Weaknesses in risk controls can arise from individual actions or systemic issues, such as poor design, and can align to cause serious consequences, as illustrated by Reason's Swiss cheese model. Normal variation in work as done vs work as imagined as described by Hollnagel (2017), can also create an incident. AI systems can also fail, and relevant taxonomies building on Reason (1997) have been suggested, Cummings (2024). These taxonomies should be explored to ensure structured learnings from AI accidents, and to avoid using "AI-Error" as a root cause. Bow-tie analysis is the suggested method used to identify preventive and reactive controls to enhance safety. Key MHC issues of local control/risk control needed to be checked are related to Human Factors Engineering:

- Is management of change performed, and work as done checked vs work as imagined in safety critical areas?
- Has a Safety Critical Task Analysis been used in design as a basis for flow of SA, HMI, Bowtie, Organization, Procedures and Layout?
- Has alarm been designed based on a best practice standard such as EEMUA 191?
- Can situations be assessed "at a glance", building on High Performance HMI design?
- Has workload analysis been done to handle stress, boredom, fatigue and mental workload?
- Is noise, lightning, temperature and work environment (ergonomics) designed in line with best practices?
- Has systematic user testing been performed on relevant data, including deviations and edge conditions?
- Has user selection and training been performed based on operational design domain and need for competence as result from the SCTA.

Exploration of Design issues: When exploring accidents a significant cause may be poor design, as described by Kinnersley et al. (2007), Moura et al. (2016), estimating that 40-50% of accidents are due to poor design. In Norman (2013) the statement is "*Human Error? – No, poor Design*" arguing and documenting that many errors or accidents are due to poor design of systems. Design as a root cause is difficult to estimate due to great variance in the quality of accident investigations. Therefore, we need better investigations standards. "Human Error" has often been used to explain 80% of accidents in shipping, however this is a misconception, no scientific basis can be found to substantiate this, Wróbel (2021). "Human Error" is a starting point for identifying systemic issues, Dekker (2017). In a discussion between the author and Don Norman, we assumed as a starting point that 80% of all accidents are due to poor design. However, root causes are often complex and involve multiple factors. In addition, it can be useful to analyse if the accident could have been avoided through elimination, substitution or engineering design. Key issues from good practice of design that should be explored are:

- Is there a Project definition, an operational domain design/ scope decision that supports and discusses MHC, such as adapted Fitts list, De Winter et al. (2014) so that we know that the system scope/ human readiness level (HRL) and TRL has been assessed, Johnsen & Aminoff (2024)?
- Has the design of the system been based on user centred design process, such as ISO 9241-210 or ISO 11064?
- Organisational and design issues: Has the Hierarchy of Controls been used actively in designing and mitigating safety challenges: prioritizing elimination, substitution, engineering controls, administrative controls?

In this section, we highlighted the need for going behind Human Error as cause document events and how the involved actors understood the incident (SA of actors), issues of local and risk control, and analyse quality of human-centred design. Existing practices in accident investigation varies and does often stop when identifying "Human Errors". There is a need to improve practice and establish an international standard for accident investigation including the science of HF, to improve learning and MHC.

4. Validity/Credibility

The paper has been based on empirical and theoretical research, the suggested elements of MHC has been based on a broad-based interview of HF experts and are in line with HF literature and best practice (i.e. member checks) and draws upon experience through prolonged engagement in the industry.

5. Conclusion and further work

MHC in digitalization, automation/AI, and remote oversight, is an ability that can be designed into a MTO system. However, MHC is a result of a learning cycle, as mentioned in the three research questions, i.e.

1)design issues, 2)operational issues and
3) ability to learn and improve from incidents.

Learning from incidents must explore missing/poor design and poor HF or HFE in operation. Thus, we need to use a systematic accident investigation method such as from NSIA (2022) or ATSB (2007).

However, we need to improve HF based methods and standards for accident investigation, that checks the quality of HF methods and HFE practices used in design and operations. The benefit of an international standard used across different industries could increase leaning and best practices.

Establishment of MHC is dependent on prioritizing HF methods and HFE techniques from the start of project, and control maturity (by assessing TRL/HRL). Thes issues should also be explored in MoC in the maintenance phase.

In the following we have listed key issues, that will be incorporated into a good practice methodology called CRIOP, Aas et al. (2009). In addition, we see the need to establish an international standard for accident investigation exploring design, HF and MHC that could be used in different industries.

Key design issues to support MHC

Setting the stage through regulation, using best practices development processes or MoC supported by techniques and guidelines to establish the foundation of MHC. Key issues are:

- Utilizing relevant best practice from aviation. Regulation that prioritizes HF and supports just culture with open reporting of incidents (prioritizing the hunt for knowledge vs the hunt for scapegoats- you must choose one approach).
- A conscious MTO scoping decision, having a Project Definition and MoC analysis, identifying key challenges and suggested approach based on an MTO perspective. Using TRL and HRL in an appropriate manner.
- A user centred design process based on good practices such as ISO 9241-210, ISO 11064.
- Systematic Human Factors Engineering based on SCTA, and design of alarms based on best practice EEMUA 191. Control workload (cognitive and physical), fatigue, boredom and circadian rhythm. Especially when tasks and workload are shared between operators and suppliers.
- Procedures and training based on user involvement and understanding of critical tasks through SCTA.
- Design of information systems based on key principles from ecological system design. Performing work domain analysis, designing the system based on the work environment and task demands, documented through SCTA and flow of situational awareness. Users should see and understand system constraints directly without needing excessive mental effort i.e. “Situation at a glance”. Visual representation of possible actions (affordances), supporting and guiding users toward appropriate decisions.
- Systematic testing, including user testing of defined situation of hazards should be performed.

Key Operational issues to support MHC

An operational environment adhering to human limitations, especially time to establish situational awareness. Key issues are:

- Controlling the chain of suppliers, taking care of the “See-To” responsibility and perform MoC.
- Necessary SA for the involved operators i.e. tasks should be supported by information systems or alarms giving the operator necessary SA. Time to handle unexpected situations, should be assessed (typical from 10 minutes to 2 minutes for an operator). Ability to handle a deviation or alarm should be based on standards. Operators should not be blamed, especially if there poor systems/training or less than 3-10 minutes to get to understand a new situation.
- Error traps, examples as listed by Norsk Industri (2023), are avoided in design and identified and handled in operations. Incidents in operations are reported, analysed and mitigating actions are implemented in collaboration with the workforce, avoiding blame. Necessary training is given.

Key Learning issues to support MHC

Learning from incidents and accidents must be based on exploring and understanding why the involved actors acted as they did. Analysis of design must check (ex. CRIOP) if good practice human factors engineering techniques was used, in addition to use of recognized human-centred methods.

- Prioritizing a learning environment build on regulation that support just culture as mandated by EU.
- Exploring and trying to understand the reasons for the actions of the operators in the sharp end. Human Error is only a starting point for identifying system challenges.
- Using a systematic accident investigation method such as from NSIA (2022) or ATSB (2007).
- Examining the influence of design decision and issues on the accident from project definition through deviations from user centred design. Use The Hierarchy of Controls active to understand and to prioritize mitigating actions.

Acknowledgements

This research has been funded by the MAS project, NFR:326676.

References

Aas, A. L., Johnsen, S. O., & Skramstad, T. (2009). CRIOP: a human factors verification and validation methodology that works in an industrial setting. In Computer Safety, Reliability, and Security: SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009. Proceedings 28 (pp. 243-256). Springer Berlin Heidelberg.

Amalberti, R. (2017). The paradoxes of almost totally safe transportation systems. In Human Error in Aviation (pp. 101-118). Routledge.

ANSI/HFES (2021). Human Readiness Level Scale in the System Development Process. (ANSI/HFES 400-2021).

ANSI-American National Standards Institute, 2012. Occupational Health and Safety Management System. ANSI/AIHA Z10, 2012. American Industrial Hygiene Association, Falls Church, VA.

Antonsen S., Ramstad L. and Kongsvik T., (2007) “Unlocking the organization: Action research as a means of improving organizational safety”, Safety Science Monitor, vol. 11(1).

ATSB (2007) Australian Transport Safety Bureau Aviation Research and Analysis

Bainbridge, L. (1983). Ironies of automation. In Analysis, design and evaluation of man–machine systems (pp. 129-135). Pergamon.

Begnum, M. E. N. (2021). 11 User-Centred Agile. Sensemaking in Safety Critical and Complex Situations Human Factors and Design, 173.

Behm, M., Culvenor J., and Dixon, G. "Development of safe design thinking among engineering students." Safety Science 63 (2014)

Bergh, L. I. V., Teigen, K. S., & Dørum, F. (2024). Human performance and automated operations: a regulatory perspective. Ergonomics, 67(6), 744–758. https://doi.org/10.1080/00140139.2024.2321457

Bjerkebaek, E., & Eskedal, T. S. (2004). Safety Assessment of Alarm Systems on Offshore Oil and Gas Production Installations in Norway. In SPE OnePetro.

Bjørneseth, F. B. (2021). Unified Bridge–Design Concepts and Results. Sensemaking in Safety Critical and Complex Situations, 135-153.

Bradshaw, J. M., Hoffman, R. R., Woods, D. D., & Johnson, M. (2013). The seven deadly myths of" autonomous systems". IEEE Intelligent Systems, 28(3), 54-61.

Briwa, H., Leva, M. C., & Turner, R. (2022). Alarm Management for human performance. Are we getting better? ESREL 2022.

Calvert, S., Johnsen S., and Ashwin. (2024). "*Designing automated vehicle and traffic systems towards meaningful human control*." In Research Handbook on Meaningful Human Control of Artificial Intelligence Systems, pp. 162-187. Edward Elgar.

Cummings, M. L. (2024). *A Taxonomy for AI Hazard Analysis.* Journal of Cognitive Engineering and Decision Making,

Dekker, S. (2017). *The field guide to understanding 'human error'.* CRC press.

De Winter, J. C., & Dodou, D. (2014). Why the Fitts list has persisted throughout the history of function allocation. Cognition, Technology & Work.

Dyreborg, J., et al., (2022). Safety interventions for the prevention of accidents at work: A systematic review. Campbell systematic reviews, 18(2), e1234.

EU/AI-The Artificial Intelligence Act - Regulation (EU) 2024/1689

EU Regulation 376/2014 reporting, analysis and follow-up of occurrences in civil aviation

EEMUA - The Engineering Equipment and Materials Users Association (EEMUA). (2024). Alarm systems: A guide to Design, Management and Procurement. (Standard No. 191).

Endsley, M.R. & Jones, D: Designing for Situation Awareness. CRC Press, Taylor & Francis, Boca Raton, Florida, 2012, 2nd edition

Energy Institute. (2020). Guidance on human factors safety critical task analysis. Energy Institute.

Equinor (2024) Presentation at the drilling conference in Kristiansand

Greenwood, D. J., & Levin, M. (2006). Introduction to action research: Social research for social change. SAGE publications

Havtil (2025) - https://www.havtil.no/en/regulations/acts/about-the-regulations/

Hancock, P. A. (2021). Months of monotony–moments of mayhem: Planning for the human role in a transitioning world of work. Theoretical Issues in Ergonomics Science, 22(1), 63-82.

Hendrick, K., & Benner, L. (1986). Investigating accidents with STEP (Vol. 13). CRC Press.

Helgar, S. "User Centered Design", retrieved from https://www.sintef.no/globalassets/project/hfc/documents/03-helgar-stein.pdf

Hollifield, et al. (2008). The high performance HMI handbook: Houston: Pas.

Hollnagel, Erik (2017). Safety-II in practice: Developing the resilience Potentials. Routledge.

HSE (2015) Literature review: Barriers to the application of Human Factors/ Ergonomics in engineering design – retrieved from https://www.hse.gov.uk/research/rrpdf/rr1006.pdf

IEA (2000)- International Ergonomics Association, retrieved at 2025.01.20 from https://iea.cc/about/what-is-ergonomics/

IEC- International Electrotechnical Commission 63303:2024 Human machine interface for process automation systems

IEC- International Electrotechnical Commission 62682:2022 Management of alarm systems for process industries

ISO -International Organization for Standardization 11064 (1999-2013). Ergonomic design of control centres.

ISO -International Organization for Standardization 9241-210 (2019). Human-centred design for interactive systems

IOGP (2017) Report 423 – HSE management – guidelines for working together in a contract environment

IOGP (2024) Report 656 – Assessment of eye tracking technology in well control operations - onshore

Johnsen, S. O., Thieme C.A., and Myklebust, T.. "Experiences Of Safety And Reliability In Remote Control Of Safety Critical Operations "(2024a). ESREL 2024 Contributions Part 5:

Johnsen, S. O., & Aminoff, H. (2024). Use of ANSI/HFES Human Readiness Level to ensure safety in automation. Human Factors in Design, Engineering, and Computing, 159(159).

Johnsen, S. O., & Winge S.. "Human Factors and safety in automated and remote operations in oil and gas: A." (2023), ESREL.

Kinnersley, S., & Roelen, A. (2007). The contribution of design to accidents. Safety Science, 45(1-2).

Kirwan, B. "Human Factors Requirements for Human-AI Teaming in Aviation." (2025).

Leva, M. C., Naghdali, F., & Alunni, C. C. (2015). Human factors engineering in system design: a roadmap for improvement. Procedia Cirp, 38, 94-99.

Lie, J.A.S, et al.. (2014). Arbeidstid og helse. Oppdatering av en systematisk litteraturstudie. (STAMI Rapport Nr. 1).

Manuele, F. A. "Risk assessment & hierarchies of control." Professional safety 50, no. 5 (2005): 33

Mecacci, G., Amoroso D., Siebert, L.C. Abbink, D. Jeroen van den Hoven, and Filippo Santoni de Sio, eds. (2024) *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems.* Edward Elgar Publishing.

Meshkati, N. (2006). Safety and human factors considerations in control rooms of oil and gas pipeline systems: conceptual issues and practical observations. International journal of occupational safety and ergonomics, 12(1), 79-93.

Miranda, A.T. (2019) Misconceptions of human factors concepts, Theoretical Issues in Ergonomics Science, 20:1, 73-83,

Moura, R., Beer, M., Patelli, E., Lewis, J., & Knoll, F. (2016). Learning from major accidents to improve system design. Safety science, 84, 37-45.

NAS - National Academies of Science (2021) Human-AI Teaming: State of the Art and Research Needs (2021).

NTSB (2010) National Transportation Safety Board. 2010. Aircraft Accident Report NTSB/AAR-10 /03. Washington, DC.

NIOSH (2024) - National Institute for Occupational Safety and Health at 2025.01.20 from - https://www.cdc.gov/niosh/hierarchy-of-controls/about/index.html

Norman, D. (2013). The design of everyday things: Revised and expanded edition. Basic books.

Norsk Industri (2023) A practical guide to HOP from www.norskindustri.no/siteassets/dokumenter/hms/hop/hop-veileder-engelsk-2024-3005.pdf

NSIA (Norwegian Safety Investigation Authority (2022) Human Factors in the NSIAs safety investigations.

Park, J. et al. "Challenges and opportunities in remote operations of automated passenger ferries identified using the CRIOP method" in press, presented at ESREL 2025.

Porathe, S. T. (2023). Alarm and hand-over concepts for human remote operators of autonomous ships. In Proceedings of ESREL 2023)

PSA (2022) #992923 Responsibility, competence, and maintenance of alarm systems in control rooms.

PSA (2019) Report "Investigation of collision between Sjoborg supply ship and Statfjord A on 7 June 2019"

Reason, J. (1997). Managing the risks of organizational accidents. Aldershot, England: Ashgate.

Safety forum -Sikkerhetsforum (2019) Learning from incidents/Rapport fra Sikkerhetsforum

Sandhåland, H., Oltedal, H., & Eid, J. (2015). Situation awareness in bridge operations study of collisions between attendant vessels and offshore facilities in North Sea. Safety science, 79, 277-285.

Skipssikkehetsloven(2007) /lovdata.no/dokument/NL/lov/2007-02-16-9

Smith, L., Folkard, S., & Poole, C. J. M. (1994). Increased injuries on night shift. The Lancet, 344(8930), 1137-1139

Stanton, Neville A., et al. Human factors methods: a practical guide for engineering and design. CRC Press, 2017.

van Winsen, R., & Dekker, S. W. (2016). Human factors and the ethics of explaining failure. In Human Factors and Ergonomics in Practice: Improving System Performance and Human Well-Being in the Real World (pp. 65-76). CRC Press.

Walker, G. H., Waterfield, S., & Thompson, P. (2014). All at sea: An ergonomic analysis of oil production platform control rooms. International Journal of Industrial Ergonomics, 44(5), 723-731.

Wróbel, K. (2021). Searching for the origins of the myth: 80% human error impact on maritime safety. Reliability Engineering & System Safety, 216, 107942.

Yasseri, S., & Bahai, H. (2018). System readiness level estimation of oil and gas production systems. International Journal Of Coastal, Offshore And Environmental Engineering (ijcoe), 3(2), 31–44