Assurance of Software-Intensive Medical Devices: What About Mental Harm?

Jose Luis de la Vara
Universidad de Castilla-La Mancha
Albacete, Spain
joseluis.delavara@uclm.es

Barbara Gallina
Mälardalens universitet
Västerås, Sweden
barbara.gallina@mdu.se

Antonio Fernández-Caballero
Universidad de Castilla-La Mancha
Albacete, Spain
antonio.fdez@uclm.es

Jose Pascual Molina
Universidad de Castilla-La Mancha
Albacete, Spain
josepascual.molina@uclm.es

Arturo S. García
Universidad de Castilla-La Mancha
Albacete, Spain
arturosimon.garcia@uclm.es

Clara Ayora
Universidad de Castilla-La Mancha
Albacete, Spain
clara.ayora@uclm.es

***Abstract*—Interdisciplinary synergies are arising from the growing usage of software, e.g., between dependability assurance and mental health. In a context in which software-intensive medical devices are used for the treatment of mental illnesses such as schizophrenia, it is important to consider mental harm when dealing with and justifying system dependability. However, we are not aware of any publication on system assurance that has paid attention to mental harm in detail. This emerging idea should be considered for the success of the devices. We discuss why and how mental harm should be addressed for assurance of software-intensive medical devices, considering hazard and risk analysis, system compliance, dependability justification, and assurance evidence collection. We draw from prior more general work and from system examples for which mental health plays a major role.**

Keywords—software-intensive systems, medical device, system assurance, system dependability, system safety, mental health, mental harm

I. INTRODUCTION

Software plays a major role and its use is increasing nowadays in many domains and interdisciplinary contexts, including critical ones such as transport and healthcare. The assurance of software-intensive systems needs to be addressed in a wider range of critical applications. Assurance can be defined as the set of activities to provide adequate justified confidence that a system satisfies given requirements, e.g., for system safety, thus for system dependability [10]. This is usually conducted according to standards and leads to certification.

Software-intensive systems are currently used in situations in which mental health is especially relevant, resulting in interdisciplinary synergies between dependability assurance and mental health. An example is medical devices [27] for the treatment of illnesses such as schizophrenia (SCZ) or autism spectrum disorder (ASD). The range of possible negative mental impacts is broader for these systems, and the possible impact on mental health of, e.g., system failures or an improper design should be considered for assurance. Otherwise, an illness or its treatment could get worse. However, issues with, e.g., mental health apps have been reported regarding reliability or usage resulting in inadequate care [31]. There are concerns about their effectiveness [45] and assurance [3]. In addition, as the number of people with mental illnesses is growing [47], a larger use of devices for mental health can be expected, e.g., to overcome human resource scarcity. Different studies [2][17] [30][49] have also reported problems and failures of medical devices due to inadequate software engineering and assurance practices.

Despite its importance, we are not aware of any publication on system assurance that has addressed mental harm explicitly and in detail. Mental harm can be defined as injury or damage to the mental health of people [28]. When dealing with safety, physical harm is the focus. If mental harm is not considered, assurance risks [9] will arise, as a developer will most likely be incapable of (1) developing a system that can be deemed dependable, (2) adequately collecting and managing assurance evidence, or (3) making a third-party (e.g., assessor) gain sufficient confidence in system dependability. Characterizing how to address mental harm represents a research challenge for the success of certain software-intensive medical devices.

We aim to provide new insights into the emerging idea of why and how mental harm should be considered for assurance of software-intensive medical devices. We build on prior work on system assurance and on concrete system examples to determine assurance needs. Although we focus on healthcare systems, the insights provided can be useful for other systems in which mental health is relevant, e.g., systems that monitor people in stressful situations. Our ultimate goal is to increase the awareness of the need to address mental harm for system assurance, as a way to encourage and contribute to the research on this topic. This work has been conducted in the scope of the ETHEREAL project (Emotional Technologies for Mental Health based on Physiological, Perceptual and Behavioural Responses) [13], in which ICT researchers, psychologists and psychiatrists collaborate to provide new mental health therapies. Such a collaboration is not frequent and, to the best of our knowledge, has not been enacted to consider mental harm for assurance of software-intensive medical devices.

II. Background

As background of the paper, we introduce some concrete examples of systems for which mental harm should be considered for their assurance. We also review related work.

A. System Examples

Mental health aspects are or can be relevant for software-intensive systems for different applications and contexts, from systems for healthcare [38][45] to more general systems that exploit artificial intelligence (AI) [8] or affective computing [48]. We focus on systems that can be used, as a part of a therapy, in rehabilitation programs for patients suffering from facial affect recognition deficits. They are software-intensive medical devices for mental health. The patients can correspond to people with SCZ, bipolar disorders (BPD), major depression disorder (MDD), or ASD. The systems can monitor people and study the mental operations involved in social interactions, including processes of perceiving, interpreting, and generating responses to the intentions, dispositions, and behaviors of others.

An example is a system for emotion recognition based on physiological, perceptual, and behavioral responses [22] for patients with SCZ, BPD, or MDD. The system can exploit electroencephalographic signals, physiological signals, and near-infrared spectroscopy. Facial or speech emotion recognition, emotion recognition based on gesture, and multimodal emotion recognition can be useful as well.

Extended reality (XR) can also be used for emotion induction and recognition [21] for patients with SCZ, BPD, or MDD. The systems can employ emotional haptic interfaces, emotion induction procedures, multimodal emotion recognition, adaptive emotional environments, and neurobiofeedback.

Another example is a system for emotion induction and recognition using social robots [41]. The system can be used for children with ASD. These systems can deal with emotion induction procedures, emotion learning by mimicry, multimodal emotion recognition, adaptive social robot emotions and behaviors to match human emotions, and neurofeedback.

As shown, there are different alternatives for the rehabilitation programs, with different technologies, elements, human-computer interaction, and automation levels. For each alternative, the assurance needs and possible mental harm can vary, but they are important in all the alternatives and share characteristics. In some cases, and although doctors support the solutions, the patients might be reluctant to use the devices. This could lead to patients leaving a rehabilitation program. System developers should ensure that a patient's mental condition will not be negatively affected because of system usage or system failure. It is also important to note that most of the system types above are results of research projects for new therapies.

B. Related Work

Assurance of software-intensive systems has been a relevant research area for decades. Among its general characteristics, both researchers [36] and practitioners [37] have acknowledged that assurance of new technologies is challenging. For such technologies, many advocate the use of assurance cases to provide structured justifications of system dependability [40]. In the healthcare domain, it has been argued that its assurance practices need to mature [44], especially when considering how they are in other application domains, and that these practices can benefit from the use of assurance cases [11].

We are not aware of any publication that has dealt with mental harm explicitly and in detail for system assurance. Without such publications, there is no evidence that mental harm has been carefully considered in the literature or in practice when addressing assurance of software-intensive medical devices. Nonetheless, some studies provide useful insights.

Ge et al. [23] worked on representing and communicating clinical reasoning with assurance cases. This study is close to what we understand that could have been addressed about mental harm. It includes an assurance case for diagnosis of attention deficit hyperactivity disorder that refers to the observation of abnormal behaviors. Salisbury [42] analyzed the compliance needs of virtual reality systems for remote therapy and patient monitoring. He referred to systems for mental health but did not analyze their needs in depth. He also stated that compliance will be necessary for these systems and that making developers aware of compliance needs will be beneficial.

A framework for the evaluation and selection of mental health mobile apps has been proposed recently [1]. Two of the criteria are approval by authorities and if it is considered that an app could harm users. Although the framework provides a basic checklist to gain confidence in a mental health app, it does not define a system assurance approach as such. For example, the framework does not deal with concrete engineering aspects, compliance needs, or potential mental harms.

Other medical devices for which assurance cases have been published include infusion pumps [4], automated external defibrillators [39], and electronic prescribing systems [29]. Recent publications have also addressed assurance case development for medical devices that exploit machine learning [5]. Authors working on assurance cases in healthcare have reported needs and areas of improvement related to hazard analysis and organizational support for assuring safety [25], and to education and guidance for healthcare stakeholders [43].

Regarding different system types, Bahaei et al. [7] proposed a framework for risk assessment of augmented reality-equipped systems and applied it in automotive. The XRSI initiative [46] has defined a framework that addresses XR privacy and safety and plans to work with medical XR. In addition, XRSI has indicated the need to consider impact on mental health in, e.g., the context of the metaverse, and the need for safety and security standards in XR environments. The need to address such quality concerns has been acknowledged for many systems and technologies, such as Internet of Things [32], AI [19], robots [36], emotion recognition with wearable devices [35], and facial recognition [33]. Specific assurance means should be defined.

III. Consideration of Mental Harm for Assurance of Software-Intensive Medical Devices

There exist four main areas to address to properly consider mental harm for assurance of software-intensive medical devices: Hazard and Risk Analysis, System Compliance, System Dependability Justification, and Assurance Evidence Collection. They are related, and it is essential to address all of them properly and jointly to avoid or mitigate assurance risks.

The need to deal with these areas applies to any safety-critical system, but doing it for software-intensive medical devices and considering mental harm requires that attention is paid to specific needs in addition to general ones. It is widely accepted that new or different technologies, as well as new or different technology usages, have distinct assurance needs [10][36][37]. We discuss such needs in the scope of mental harm for assurance of software-intensive medical devices, also mentioning solutions to address the needs.

A. Hazard and Risk Analysis

A key activity during the whole lifecycle of any critical system is to analyze, estimate, and control the possible hazards (sources of harm [28]) that can affect it. For mental health therapies, a medical device might cause some negative impact on mental health (e.g., an undesired emotion), not detect some possible mental harm, make a patient deviate from the expected therapy (e.g., the patient distracts), or make a patient reluctant to follow a treatment. For the systems referred to above, emotion induction arguably requires especial attention. Mental health professionals need to participate in this activity, providing insights into and feedback on the possible harms.

At early lifecycle stages, conditions that can lead to mental harms must be determined, e.g., with fault tree analysis. When decisions are made about how a medical device will be, the possible negative impacts of system elements need to be studied, e.g., with failure mode and effect analysis. The harms must also be assessed to determine risk levels, which must be acceptable. System requirements that address the risks must be specified.

There are many aspects that the possible solutions need to consider to adequately analyze a system from a mental harm perspective, such as envisioned functionality, user interaction, expected usage, possible misuse, usability, and automation level, as well as requirements and input from ethics committees. Since the systems are typically built from existing components, the extent to which the components are reliable is important. Their available dependability information (e.g., usage warning information) and manuals are also important. Differences among patients, e.g., adults and children or according to their illness [16], must be taken into account. Aspects that are gaining attention and are relevant include multi-concern assurance (e.g., of safety, security, and privacy) [20], human-computer interaction failures [6], and AI trustworthiness [12].

B. System Compliance

Critical systems, including medical devices, usually must comply with assurance and engineering standards to be allowed to operate [24]. This might not be compulsory for software-intensive medical devices involved in new therapies or from research projects, but it is still important that developers and other stakeholders are aware of the standards. It is also important to note that, e.g., EU Regulation 2017/745 [14] indicates that medical device software shall be developed in accordance with the state of the art. The main point is not that compliance is sought, but that the stakeholders gain awareness of best practices and recommendations that can make the devices more dependable and contribute to mental health assurance.

The parts of a standard applicable to a device will depend on its risk level, thus on Hazard and Risk Analysis results. For example, the IEC 62304 standard for medical devices [27] indicates that software safety will be categorized as no injury or damage to health is possible, non-serious injury is possible, or death or serious injury is possible. For the system examples that we use, we argue that injuries are possible. This dictates how rigorous the software lifecycle should be. For example, unit, integration, and system testing should be conducted. This is not the case when no damage is possible. System compliance solutions also need to pay attention to software reuse, and especially to software of unknown provenance.

Another standard that we regard as relevant is ISO 14971 [28], which defines practices for risk management of medical devices. This includes specification of risk acceptance principles [18], in line with the description of the Hazard and Risk Analysis area. Depending on the characteristics of a medical device, other standards might be relevant, from healthcare or other domains such as robotics, and considering software and non-software aspects. Interaction compliance [19] can be relevant as well.

An aspect into which we would like to gain insights is whether and, if so, how standardization committees have taken mental health into account when defining standards. This is uncertain to us. For instance, the definition of harm in IEC 62304 refers to “physical injury, damage, or both to the health”, but “physical” is not used in the definition in ISO 14791. Mental impairment is acknowledged as a possible consequence of a serious adverse event in EU Regulation 2017/745.

In the US, FDA guidance and reference documents have referred to, e.g., mobile apps for mental health [15]. Nonetheless, clear guidance is missing regarding which apps are or are not considered medical devices, as well as other policies [1]. We have found examples of mental health apps that have sought FDA approval [26] and some apps have obtained it [34]. However, such approvals appear to have been based on treatment effectiveness supported by scientific evidence from clinical studies, rather than on adherence to acceptable software engineering and assurance practices. This is also necessary.

Last but not least, concerns have been raised about who will or should regulate mental health technology and the data that it generates, and from the fact that there are no standards to know if such technology is proven to be effective [45]. Solutions that define how the corresponding systems should comply with standards will contribute to tackling these concerns.

C. System Dependability Justification

From our experience in and knowledge about projects on software-intensive medical devices for mental health, system dependability justification is an area of which most stakeholders are not aware. Therefore, general considerations need to be introduced to them, in addition to mental harm-specific ones.

Once mental health risks and compliance needs have been determined, it is important to provide explicitly a justification of why and how the risks have been addressed and why and how compliance has been achieved. In the scope of assurance cases, such justifications can be referred to as risk (or hazard management) argument and compliance argument [11]. In addition, confidence arguments can be important to justify why someone should trust the other two arguments. Both process-based and product-based aspects might need to be considered.

It is also relevant that stakeholders understand that system dependability justification evolves and needs to be addressed throughout a system's lifecycle [11], the same as hazard and risk analysis. Versions of assurance cases could be developed and maintained at system concept, specification, implementation and V&V, deployment, operation, and decommissioning stages.

For mental health, we think that ethics aspects need to be considered as well as a part of the solutions for dependability justification, e.g., with some kind of ethical argument [8]. This is aligned with the review and approval, by ethics committees, of new therapies and of the use of new medical devices. Such reviews and approvals require several cycles, which is in turn aligned with the need for assurance cases that evolve. Ethics aspects can even be more important for AI-based systems [12].

A specific solution that can help system developers provide the needed justifications is argument patterns [23]. The patterns define the overall, generic, and abstract structure of a dependability justification that could be regarded as valid. The developers can use the patterns as a reference to build concrete argument instances for their systems. We are not aware of any argument pattern that deals with mental harm of medical devices. For some medical devices, argument patterns on the usage of machine learning can be useful.

Finally, as the medical devices involved in mental health therapies usually reuse existing components, proven-in-use arguments [36] can play an important role. Such arguments justify why a system or component can be deemed dependable based on its past operation. If sensors and XR devices have not failed in the past, then their trustworthiness can be argued.

D. Assurance Evidence Collection

Assurance evidence can be defined as artefacts that contribute to developing confidence in the dependable operation of a system and to showing the fulfilment of the requirements of assurance standards [37]. Examples of artefact types that can be used as assurance evidence include system analysis results, system specifications, and V&V results. Assurance evidence supports system dependability justification and compliance.

There are several aspects of assurance evidence collection that need to be addressed in the solutions for consideration of mental harm for system assurance. The first aspect corresponds to what artefact types [37] might be more relevant. Because of the characteristics of the devices, how they are built, and how they are used, as well as of how new therapies are approved, process information seems especially important, such as system inception specification, project management plans, activity records, operation procedures, reused component specification, reused component historical service data specification, and operator competence specification. A thorough characterization of the patients that will use a system, of their expected mental condition, of usage steps, and of training needs can be essential.

The second aspect is where to collect evidence data from. Several heterogenous sources and formats should be involved, including sensors that monitor patients, forms with which patients and mental health professionals that observe the patients provide feedback, mental health professionals that conduct some (early) system validation, and approvals from ethics committees, in addition to the typical engineering sources. As the development and initial use of a medical device progress, and depending on the extent to which and where the device will be deployed, results from clinical studies might be necessary.

Another aspect is how assurance evidence evolves, the same as assurance cases should do. This is also in line with the multiple approvals from ethics committees that can be required for new therapies and for the medical devices used.

The last aspect is evidence trustworthiness. For example, the patients that participate in new therapies are typically volunteers eager to use new devices and be informed of an improvement in their state. This might threat the validity of their feedback. It is important to note that, for certain therapies, the patients must be in a stable mental condition. This contributes to trustworthiness of the evidence collected from them.

IV. Conclusion

Mental harm should be considered in the assurance of many software-intensive medical devices. How to address this emerging idea needs to be determined, especially in the current situation in which software usage for mental health and the number of people with mental illnesses are growing. Otherwise, the devices might not succeed. Synergies between dependability assurance and mental health are also necessary.

We have discussed these needs and presented areas where mental harm should be considered as a part of system assurance, differently to other situations. Hazard and Risk Analysis must study what can lead to an undesired mental condition, considering specific aspects such as patient interaction, possible misuse, and requirements and input from ethics committees. System Compliance must deal with both software and non-software standards. Compliance needs will depend on how negative the consequences of, e.g., system failures could be on mental health. System Dependability Justification can benefit from different types of arguments, both common ones such as process- and product-based arguments and more mental harm-targeted types such as ethical arguments. Argument patterns that deal with mental harm of medical devices will also be valuable. Assurance Evidence Collection must take specific evidence types, formats, and sources into account, e.g., from the sensors that the medical devices use or the patients and mental health professionals that are involved in a given treatment. In essence, system developers, as well as other stakeholders, must be aware of the areas and of their needs and pay attention to them.

As future work, we plan to define specific means to deal with mental health for assurance of software-intensive medical devices. Psychologists, psychiatrists, and ICT researchers will collaborate in this activity in the ETHEREAL project.

Acknowledgment

The work leading to this paper has received funding from the ETHEREAL (MCIN/AEI ref. PID2020-115220RB-C21; ERDF), REBECCA (HORIZON-KDT ref. 101097224; MCIN/AEI ref. PCI2022-135043-2; NextGen.EU/PRTR), VALU3S (H2020-ECSEL ref. 876852; MCIN/AEI ref. PCI2020-112001; NextGen.EU/PRTR), and "Paradigmas de interacción para la nueva era de resiliencia digital" (UCLM ref. 2022-GRIN-34436; ERDF) projects, and from the Ramon y Cajal Program (MCIN/AEI ref. RYC-2017-22836; ESF).

REFERENCES

[1] S. Agarwarl, et al., "Evaluation of mental health mobile applications," Agency for Healthcare Research and Quality, 2022.

[2] H. Alemzadeh, et al., "Analysis of safety-critical computer failures in medical devices," IEEE Secur. Priv., vol. 11(4) pp. 14-26, 2013.

[3] E. Anthes, "Pocket psychiatry: mobile mental-health apps have exploded onto the market, but few have been thoroughly tested," Nature, vol. 532(7597), pp. 20-24, 2016.

[4] A. Ayoub, et al., "A safety case pattern for model-based development approach," NASA Formal Methods 2012, pp. 141-146.

[5] M. Bagheri, et al., "Towards Developing Safety Assurance Cases for Learning-Enabled Medical Cyber-Physical Systems," SafeAI 2023.

[6] S.S. Bahaei and B. Gallina, "Augmented reality-extended humans: towards a taxonomy of failures – focus on visual technologies," ESREL 2019, pp. 207-214.

[7] S.S. Bahaei, et al., "A case study for risk assessment in AR-equipped socio-technical systems," J. Syst. Archit., vol. 119, 102250, 2021.

[8] C. Burr and D. Leslie, "Ethical assurance: a practical approach to the responsible design, development, and deployment of data-driven technologies," AI Ethics, in press.

[9] J.L. de la Vara, et al., "Model-based assurance evidence management for safety-critical systems," Softw. Syst. Model., vol. 21(6), pp. 2329-2365, 2022.

[10] J.L. de la Vara, et al, "Assurance and certification of cyber-physical systems: the AMASS open source ecosystem", J. Syst. Softw., vol. 171, 110812, 2021.

[11] G. Despotou, et al., "Introducing safety cases for health IT," SEHC 2012, pp. 44-50.

[12] EC, Ethics guidelines for trustworthy AI, 2022.

[13] ETHEREAL project (online) https://www.i3a.uclm.es/louise_w/?project=emotional-technologies-for-mental-health-based-on-physiological-perceptual-and-behavioural-responses-ethereal

[14] EU, Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, 2017.

[15] FDA, Policy for device software functions and mobile medical applications: guidance for industry and Food and Drug Administration staff, 2022.

[16] M.B. First, et al., Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5), American Psychiatric Association, 2013.

[17] Z. Fu, et al., "Study of software-related causes in the FDA medical device recalls," ICECCS 2017, pp-60-69.

[18] B. Gallina, et al., "Process compliance re-certification efficiency enabled by EPF-C ∘ BVR-T," QUATIC 2020, pp. 211-219.

[19] B. Gallina, et al., "Towards explainable, compliant and adaptive human-automation interaction," XAILA 2020.

[20] B. Gallina, et al., "Multiconcern, dependability-centered assurance via a qualitative and quantitative coanalysis," IEEE Softw., vol. 39(4), pp. 39-4, 2022.

[21] A.S. García, et al., "Design of reliable virtual human facial expressions and validation by healthy people," Integr. Comput. Aided Eng., vol. 27(3), pp. 287-299, 2020.

[22] B. García-Martínez, et al., "Application of dispersion entropy for the detection of emotions with electroencephalographic signals," IEEE Trans. Cogn. Dev. Syst., vol. 14(3), pp. 1179-1187, 2022.

[23] X. Ge, et al., "Introducing goal structuring notation to explain decisions in clinical practice," Procedia Technol., vol. 5, pp. 686-695, 2012.

[24] T. Granlund, et al., "Medical software needs calm compliance," IEEE Softw., vol 39(1), pp. 19-28, 2022.

[25] I. Habli, et al., "What is the safety case for health IT? A study of assurance practices in England," Saf. Sci., vol. 110, pp. 324-335, 2018.

[26] A. Hein, "How Does the FDA Regulate Mental Health Apps?," Clarkston Consulting, 2019.

[27] IEC, IEC 62304 - Medical device software–Software life cycle processes, 2006.

[28] ISO, ISO 14971 - Medical devices - Application of risk management to medical devices, 2019.

[29] Y. Jia, et al., "Developing a safety case for electronic prescribing," MEDINFO 2019, pp. 629-633.

[30] R. Kitawaki, et al., "Analysis of medical device recalls owing to output information from software," Regulatory Science of Medical Products, vol. 6(3), pp. 281–293, 2016.

[31] C. Lane, "Digital health and the rise of mental health apps," Psychology Today, 2018.

[32] P.A. Laplante,et al., "Building caring healthcare systems in the Internet of Things," IEEE Syst. J., vol. 12(3), pp. 3030-3037, 2018.

[33] D. Leslie, Understanding bias in facial recognition technologies. The Alan Turing Institute, 2020.

[34] A. Marschall, "Which Mental Health Apps Are FDA-Approved?," Verywell Mind, 2022.

[35] J.A. Miranda, et al., "Embedded emotion recognition: Autonomous multimodal affective internet of thing," CPSWS 2018, pp. 22-29.

[36] S. Nair, et al., "An extended systematic literature review on provision of evidence for safety certification," Inf. Softw. Technol., vol 56(7), pp. 689-717, 2014.

[37] S. Nair, et al., "Evidence management for compliance of critical systems with safety standards: A survey on the state of practice," Inf. Softw. Technol., vol. 60, pp. 1-15, 2015.

[38] S.M. Preum, et al., "A review of cognitive assistants for healthcare: trends, prospects, and future directions," ACM Comput. Surv., vol. 53(6), pp. 130:1-130:37, 2021.

[39] A. Ruiz et al., "Safety case driven development for medical devices," SAFECOMP 2015, pp. 183-196.

[40] M. Sabetzadeh, et al., "A goal-based approach for qualification of new technologies: Foundations, tool support, and industrial validation," Reliab. Eng. Syst. Saf., vol. 119, pp. 52-66, 2013.

[41] M.A. Salichs, et al., "Mini: A new social robot for the elderly," Int. J. Soc. Robotics, vol. 12(6), pp. 1231-1249, 2020.

[42] J.P. Salisbury, "Using Medical Device Standards for Design and Risk Management of Immersive Virtual Reality for At-Home Therapy and Remote Patient Monitoring," JMIR Biomedical Engineering, vol. 6(2), e26942, 2021.

[43] M.A. Sujan, et al., "Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices," Saf. Sci., vol. 84, pp. 181-189, 2016.

[44] M.A. Sujan, et al., "How can health care organisations make and justify decisions about risk reduction? Lessons from a cross-industry review and a health care stakeholder consensus development process," Reliab. Eng. Syst. Saf., vol. 161, pp. 1-11, 2017.

[45] National Institute of Mental Health, Technology and the Future of Mental Health Treatment, 2021.

[46] XRSI - XR Safety Initiative (online) https://xrsi.org/

[47] World Health Organization, Mental disorders, 2022.

[48] N. Yusupova, et al., "Tools for affective computations in the management of energy facilities, considering the emotional state of operators," ICOECS 2021, pp. 233-238.

[49] Y. Zhang, et al., "User interface software errors in medical devices: study of US recall data," Biomedical Instrumentation & Technology, vol. 53(3), pp. 182-194, 2019.