Safety Science 160 (2023) 106051

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Review

Brain-computer interfaces in safety and security fields: Risks and applications

F. Brocal

Department of Physics, Systems Engineering and Signal Theory, University of Alicante, Alicante, Spain
University Institute of Physics Applied to Sciences and Technologies, University of Alicante, Alicante, Spain

ARTICLE INFO

Keywords:
Brain-computer interface
Emerging risk
Occupational
Risk
Safety
Security

ABSTRACT

With the recent increasing interest of researchers for Brain-Computer Interface (BCI), emerges a challenge for safety and security fields. Thus, the general objective of this research is to explore, from an engineering perspective, the trends and main research needs on the risks and applications of BCIs in safety and security fields. In addition, the specific objective is to explore the BCIs as an emerging risk.

The method used consists of the sequential application of two phases. The first phase is carried out a scoping literature review. And with the second phase, the BCIs are analyzed as an emerging risk.

With the first phase, thematic categories are analyzed. The categories are fatigue detection, safety control, and risk identification within the safety field. And within the security field are the categories cyberattacks and authentication. As a result, a trend is identified that considers the BCI as a source of risk and as a technology for risk prevention. Also, another trend based on the definitions and concepts of safety and security applied to BCIs is identified. Thus, "BCI safety" and "BCI security" are defined.

The second phase proposes a general emerging risk framing of the BCI technology based on the qualitative results of type, level, and management strategies for emerging risk.

These results define a framework for studying the safety and security of BCIs. In addition, there are two challenges. Firstly, to design techniques to assess the BCI risks. Secondly, probably more critical, to define the tolerability criteria of individual and social risk.

1. Introduction

Brain-Computer Interface (BCI) emerged as a technology that integrates computer systems with the human brain (Bernal, S. L. et al., 2020) quantifying central nervous system (CNS) activity and translating it into new artificial outputs that replace, restore, enhance, supplement, or improve the natural CNS outputs (Wolpaw et al., 2020). Such information can be used to control devices, artificial limbs, or obtain knowledge of (hidden) intentions (Roelfsema et al., 2018).

Landau et al. (2020) point out that BCI research began in 1973 and Bernal (2021) indicates that one of the first BCI solutions was developed at the end of the 1990 s, although it is in recent years when these devices are of increasing interest to researchers (Burwell et al., 2017; Landau et al., 2020; Li, Q. Q. et al., 2015; Ramsey, 2020) because the progressive understanding of human brain function is improving the decoding process of neural activity (Ramsey, 2020) being able to differentiate a single neuron or a small population (Bernal et al., 2020). Bonaci et al. (2015) consider that BCIs are a particular type of exocortex. Advances in machine learning have substantially improved the reliability of BCI applications, enhancing their applicability in everyday life (Merrill et al., 2019). The current technological revolution combined with the Internet of Things (IoT) is facilitating the development of specific BCIs, such as direct communications between brains known as Brain-to-Brain or Brainets and brains connected to the Internet (Bernal et al., 2021).

From an engineering perspective, a BCI is a communication system between the brain and the external environment that is configured by inputs (neuronal signal from the user), outputs (signal for the execution of commands towards the external environment), and intermediate components for acquisition and signal processing (Bonaci et al., 2015). Thus, from this engineering perspective that will be maintained throughout this work, the effective usage of a BCI device entails a closed-loop configured for three specific processes (Bonci et al., 2021; L. R. Hochberg & J. P. Donoghue, 2006): sensing, processing, and actuation (effector).

In the sensing process, the bio-electric signals are sensed through several technologies that can be classified as invasive and non-invasive

E-mail address: francisco.brocal@ua.es.

https://doi.org/10.1016/j.ssci.2022.106051
Received 1 April 2022; Received in revised form 13 December 2022; Accepted 27 December 2022

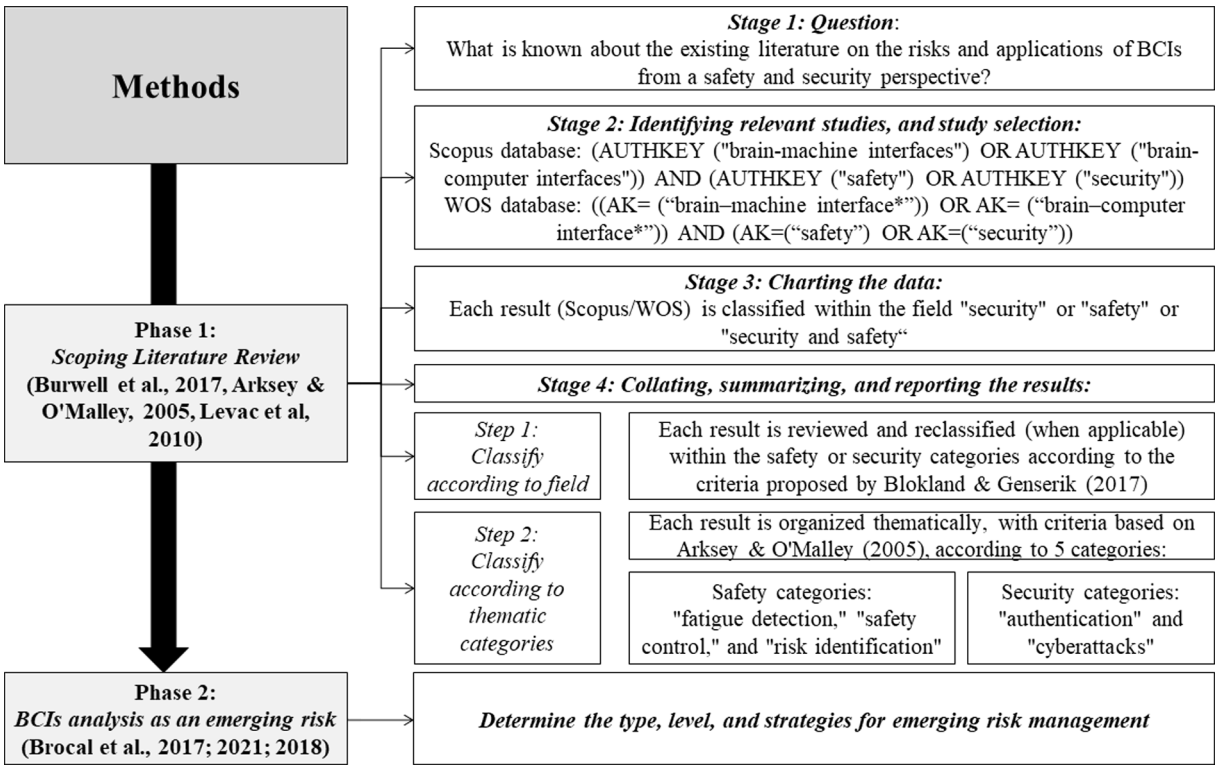

Fig. 1. Scheme of the method used.

(Bonci et al., 2021). The most used non-invasive BCIs are electroencephalography (EEG) (Li et al., 2015; Moioli et al., 2021), and the most used invasive BCIs are local field potentials (LFP) and electrocorticography (ECoG) (Moioli et al., 2021). Other possible sensors include functional magnetic resonance imaging (fMRI) systems, near-infrared (NIR) systems, magnetocencephalography (MEG), and microelectrode-based intracortical neurophysiology (L. R. Hochberg & J. P. Donoghue, 2006). Landau et al. (2020) present an interesting taxonomy of these methods and provide a comparative analysis of these methods.

In the processing process, a computing system receives neural data recorded by the sensor, discerns the user's intention, and converts that intention into a command signal for the actuator (L. R. Hochberg & J. P. Donoghue, 2006). With the actuation process the user's intention signal is translated into specific commands for a computer or robotic system to execute (Bonci et al., 2021). Proposed actuators include a cursor on a computer screen, a motorized wheelchair, a semiautonomous robot, a prosthetic limb, or a functional electrical stimulation device that could reanimate a paralyzed limb. (L. R. Hochberg & J. P. Donoghue, 2006). Finally, the cycle is closed with the feedback that the user receives to adjust their thoughts and generate new signals for the BCI system to interpret them again (Bonci et al., 2021).

The development and application of BCIs is becoming widespread due to the good results and the maturation of this technology applied in patients affected by motor paralysis (Summerer et al., 2009). In addition to improving autonomy among patients with certain motor injuries and other diseases, it is pursued that, among other applications, these devices improve cognitive functions such as memory and attention, optimize brain fitness, and control games and objects (Bonci et al., 2021; Coates McCall et al., 2019). For example, Sourin et al. (2016) point out the following research areas on applications of BCI, including real-time brain state recognition from EEG, recognition, human cognition enhancement, consumer neuroscience, and neuromarketing, human abilities assessment, and neuroscience-informed design.

These developments could allow the implantation of advanced BCIs in the future, in contexts other than therapeutic ones, which will enable reading and writing directly in the brain and therefore could be used to increase the cognitive functions of healthy individuals, being necessary for it, a detailed understanding of the neural code to minimize the loss of information and to avoid modifications of perception, thoughts, and actions are avoided (Roelfsema et al., 2018).

In this emerging context of research on BCI technologies, the number of works that address the risks and applications of BCIs in safety and security is very scarce, as well as analyzed in this research.

For example, the safety field has been discussed in the context of the unknown cognitive effects of neurostimulation (Wexler, 2020). This research context and its potential translation to therapeutic intervention (Burwell et al., 2017) identified that the most common problems are related to the safety of BCI devices and the related balance of risk and benefit to the BCI user. Furthermore, according to said authors, all this generates significant ethical, legal, and social concerns, notably about personhood, stigma, autonomy, privacy, research ethics, safety, responsibility, and justice.

Regarding the security field, Li et al. (2015) classified and studied BCI applications into the following four usage scenarios from a security and privacy perspective: neuro medical applications, user authentication, gaming and entertainment, and smartphone-based applications. Bernal et al. (2021) sing out that the development of specific BCIs increases the importance of the challenge for security (Bernal et al., 2021). For example, sensing and stimulating the brain due to implants BCI represents a fundamental challenge for security (Moioli et al., 2021).

Thus, two different trends seem to be observed but interrelated in a bidirectional way related to safety and security. These two trends evolve on the consideration of the BCI as a source of risk and technology for risk prevention.

On the other hand, the terminology used in the field of study of BCIs is still recent and not standardized, so terms such as brain-machine interfaces, brain-computer interfaces, neural interface, or neural prosthetic systems, are used interchangeably (L. R. Hochberg & J. P. Donoghue, 2006; Wester et al., 2013). In this sense, Wolpaw et al.

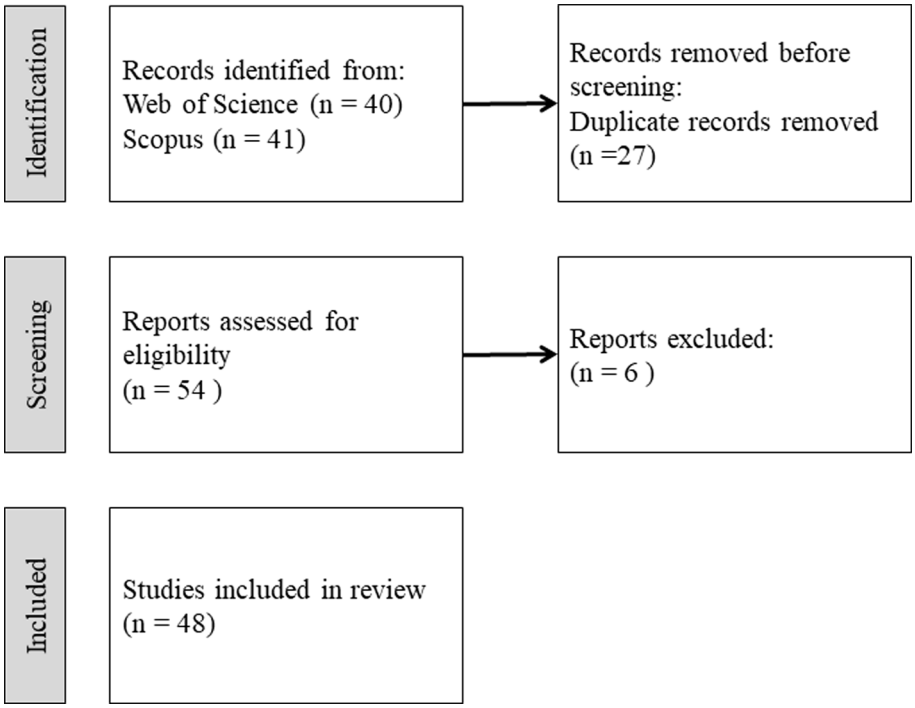

Fig. 2. Search strategy.

(2020) point out that BCIs are often called brain-machine interfaces (BMIs), although in general BCIs might be considered the preferable term. Therefore, in the present research the term BCI is used preferentially.

Thus, the general objective of this research is to explore, from a risk engineering perspective, the trends and main research needs on the risks and applications of BCIs in safety and security. And the specific objective is to explore the BCIs as an emerging risk.

The manuscript is organized as follows to achieve these objectives. First, the method used is described, consisting of a scoping literature review followed by an analysis of the BCI as an emerging risk. Second, the results are presented, beginning with the characteristics of the reviewed results, followed by a narrative account of the existing literature and the analysis of BCI as an emerging risk. Thus, the literature is organized thematically according to five different intervention types. For the safety field, three categories are identified: “fatigue detection,” safety control,“ and ”risk identification“. And for the security field, the categories ”authentication“ and ”cyberattacks“ are specified. The analysis of BCI as an emerging risk includes determining the type, level, and strategies for emerging risk management. Finally, these results are analyzed and discussed.

2. Methods

The method used consists of the sequential application of two phases. The Fig. 1 shows a scheme of the method followed by its main characteristics. With the first phase, a scoping literature review was carried out. And with the second phase, the BCIs were analyzed as an emerging risk.

A scoping literature review has been applied, for which the work by Burwell et al. (2017) has been taken as a reference as well as the works cited by said authors, specifically the method proposed by Arksey & O’Malley (2005) and the updating by Levac et al. (2010). Thus, this method has been chosen because it facilitates the process aimed at summarizing findings, exploring the extent of research on a certain topic as well as identifying research gaps. This method is configured by the following four stages: (1) identifying the research question, (2) identifying relevant studies, and study selection, (3) charting the data, and (4) collating, summarizing, and reporting the results (the five stages that initially make up the method have been reduced to four with the integration of stages 2 and 3 in stage 2).

The analysis of BCI as an emerging risk has been based on the theoretical framework proposed by Brocal et al. (2017; 2021; 2018).

2.1. Scoping literature review

1. *Identifying the research question.*

The research question for this phase was: What is known about the existing literature on the risks and applications of BCIs from a safety and security perspective?

With the answer to this question, future research associated with safety and security fields could be indicated.

2. *Identifying relevant studies, and study selection.*

Due to the multidisciplinary characteristics of the BCIs, the Scopus and Web of Science database (WOS) were selected because they are analysis tools for the world’s leading research journals and articles from virtually every specialty in science, technology, and social science. For it, “All Databases,” “All Collections,” and “All years” were selected in both cases. The search occurred in November 2021 and used the following search strings (AUTHKEY/AK = Author Keywords):

Scopus database: (AUTHKEY (“brain-machine interfaces”) OR AUTHKEY (“brain-computer interfaces”)) AND (AUTHKEY (“safety”) OR AUTHKEY (“security”)).

WOS database: ((AK= (“brain–machine interface*”)) OR AK= (“brain–computer interface*”)) AND (AK=(“safety”) OR AK= (“security”)).

Results (articles, conference, and proceedings papers) were included if they (1) were written in English (full text or abstract if it provided enough information), (2) presented conceptual discussions or empirical findings on safety or security of BCIs, (3) referred to humans, and (4) consider BCI as technology that records directly from the brain to create

Table 1
Search strings used to categorize results within security or/and safety.

Search string	Field	Scopus	WOS
Search string 1	Safety or Security	(AUTHKEY ("brain-machine interfaces") OR AUTHKEY ("brain-computer interfaces")) AND (AUTHKEY ("safety") OR AUTHKEY ("security"))	((AK=("brain–machine interface")) OR AK=("brain–computer interface")) AND (AK=("safety") OR AK=("security"))
Search string 2	Safety	(AUTHKEY ("brain-machine interfaces") OR AUTHKEY ("brain-computer interfaces")) AND (AUTHKEY ("safety"))	((AK=("brain–machine interface")) OR AK=("brain–computer interface")) AND (AK=("safety"))
Search string 3	Security	(AUTHKEY ("brain-machine interfaces") OR AUTHKEY ("brain-computer interfaces")) AND (AUTHKEY ("security"))	((AK=("brain–machine interface")) OR AK=("brain–computer interface")) AND (AK=("security"))
Search string 4	Safety and Security	(AUTHKEY ("brain-machine interfaces") OR AUTHKEY ("brain-computer interfaces")) AND (AUTHKEY ("safety") AND AUTHKEY ("security"))	((AK=("brain–machine interface")) OR AK=("brain–computer interface")) AND (AK=("safety") AND AK=("security"))

executable output. Proceedings and conference papers are included because they allow broadening the perspective of bibliographic exploration, the main objective of this research. Results excluded were if the BCI is considered in isolation or as an example and is not part of the objectives of the publication.

38 results from Scopus and 37 results from WOS were obtained after applying these criteria. On the set of these publications, duplicate articles were excluded, and results were obtained n = 48 articles for analysis (Fig. 2).

3. *Charting the data*

Information on research area and document types were obtained and categorized with Scopus and WOS analysis tools.

In turn, each result was also categorized within the field "security" or "safety" or "security and safety". For this, the previous search strings were conveniently adjusted as it is showed in Table 1.

4. *Collating, summarizing, and reporting the results*

Objectives, methodology, main measures, and results related to the safety and security of each outcome are analyzed in two steps to present a narrative account of the existing literature.

First, the results obtained with the search strings through the previous phase have been analyzed to classify them within the safety or security fields from a broad and general perspective.

Thus, the distinction between safety and security fields, the criteria considered by Blokland & Genserik (2017), have been applied. In this way, in the present research, the main distinction between security and safety is used from the perspective of the "effects of uncertainty in the objectives," considering that the effects can be regarded as "intentional" or "unintentional" (accidental). Thus, when the negative effects on the targets are "intentional," the term security is used, and when they are "unintentional," the term safety is used.

Second, the literature was organized thematically according to 5 different intervention types. Next, within each field (safety and security), the works with common themes were sought by analyzing their objectives and methodologies.

Thus, for the safety field, the categories "fatigue detection," "safety control," and "risk identification" have been identified. In the present work, the studies classified within the fatigue detection category address the detection of said fatigue, using BCI devices, when this fatigue may affect the safety of tasks such as driving or monitoring processes. In turn, mental health definition according to ISO 10075–1:2017 standard is: temporary impairment of mental and physical functional efficiency, depending on the intensity, duration, and temporal pattern of the preceding mental strain (International Organization for Standardization (ISO), 2017). Regarding the studies classified within the safety control category there are studies which address this issue through BCI devices linked to automated and robotic systems. As to the studies classified within the risk identification category there are studies which are not included in the previous categories that address, through BCI devices, the study of accident risk.

In the case of the "fatigue detection" category, the classification is relatively straightforward since the works included here have this topic in common. For example, for the category "fatigue detection," the study of mental fatigue applied to driving safety has been addressed by various authors (Liu et al., 2015; Liu et al., 2016; Min & Cai, 2020; Ming et al., 2021; Zhang, Z. T. et al., 2016). In the case of the "safety control" category, the results are not as immediate. However, the corresponding works address interventions and technologies directly linked to the said category, such as Witkowski (2014) about enhancing the reliability and safety of continuous hand exoskeleton-driven grasping motions or Penaloza et al. (2015) when the operator perceives an error made by the robot. The category "Identification of risks" has been created to include works that address risk from a general perspective since its characteristics limit a more specific classification.

For the security field, the categories "authentication" and "cyberattacks" have been identified. For both categories, the classification has also been relatively simple and direct because the corresponding results have this theme in common. For example, for the category "authentication," Narayana et al. (2019) present an application for the physically challenged consisting of a biometric security system configured by a BCI, or Merrill (2019) designed a brain-based authentication system using custom-fit EEG earpieces. And for the "cyberattacks" category, the works by Bernal et al. (2020, 2021, 2022) regarding the BCI life cycle are excellent prototypical examples of this category.

2.2. BCIs as an emerging risk

The analysis of BCI as an emerging risk will be based on the theoretical framework proposed by Brocal et al. (2017, 2018, 2021). Said theoretical framework is adequate because three reasons: (a) it allows a qualitative approach to study an emerging risk based on the evolution of its technology lifecycle (TLC); (b) uncertainty is considered the main characteristic of emerging risk; (c) this uncertainty is integrated as a combination of knowledge and understanding of the emerging risk in the mentioned theoretical framework.

Therefore, the BCI is analyzed as an emerging risk considering the importance of the current evolutionary moment of its TLC and the characteristics of the uncertainty, knowledge, and understanding of this emerging risk.

To do this, firstly, the type of emerging risk (ERi) will be defined using the models proposed by Brocal et al. (2017; 2018). Secondly, the level of emerging risk will be determined through the emerging risk classification scheme proposed by Brocal et al. (2021). Thirdly, the strategies for emerging risk management will be defined through the criteria established by Brocal et al. (2021).

3. Results

The results of the scoping literature review and the analysis of BCIs as an emerging risk are shown below. The results of the scoping literature review are composed of the bibliometric characteristics and the

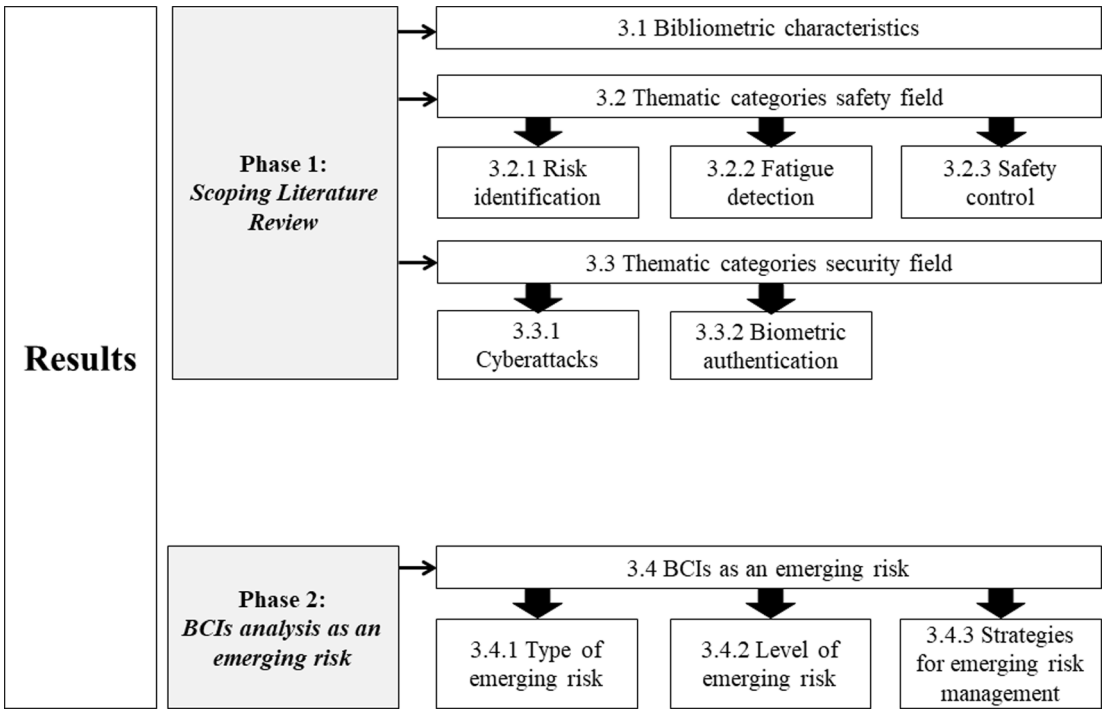

Fig. 3. Results structure.

Table 2
Final results distributed by year of publication.

Year	2009	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Results	1	1	1	1	1	4	7	4	4	6	10	7	1

Table 3
Keywords and the number of occurrences with the VOSviewer software.

Scopus Database		WOS Database	
Keyword	Occurrences	Keyword	Occurrences
Brain computer interface	35	Brain-computer interfaces	10
Electroencephalography	18	Recognition	4
Interfaces (computer)	14	Brain-computer interface	9
Brain-computer interfaces	12	eeg	5
Privacy	8	Classification	5
Security	8	Electroencephalogram	4
Human	7	Security	6
Computer privacy	6	Biometrics	4
Brain	8	Electroencephalography	7
Electrophysiology	7	Identification	4
Brain-computer interface	10	Memory	4
Data privacy	5	Privacy	6
Humans	5	Fatigue	5
Security and privacy	4	Safety	6
Article	4	Brain-computer interface (bci)	4
Security of data	5		
Brain machine interface	5		
Cyber security	5		
Authentification	4		
Electroencephalogram	4		
Biomedical signal processing	4		
Classification (of information)	4		
Safety	4		
Virtual reality	5		
Safety engineering	4		
Driving safety	4		
Electro-encephalogram (eeg)	4		

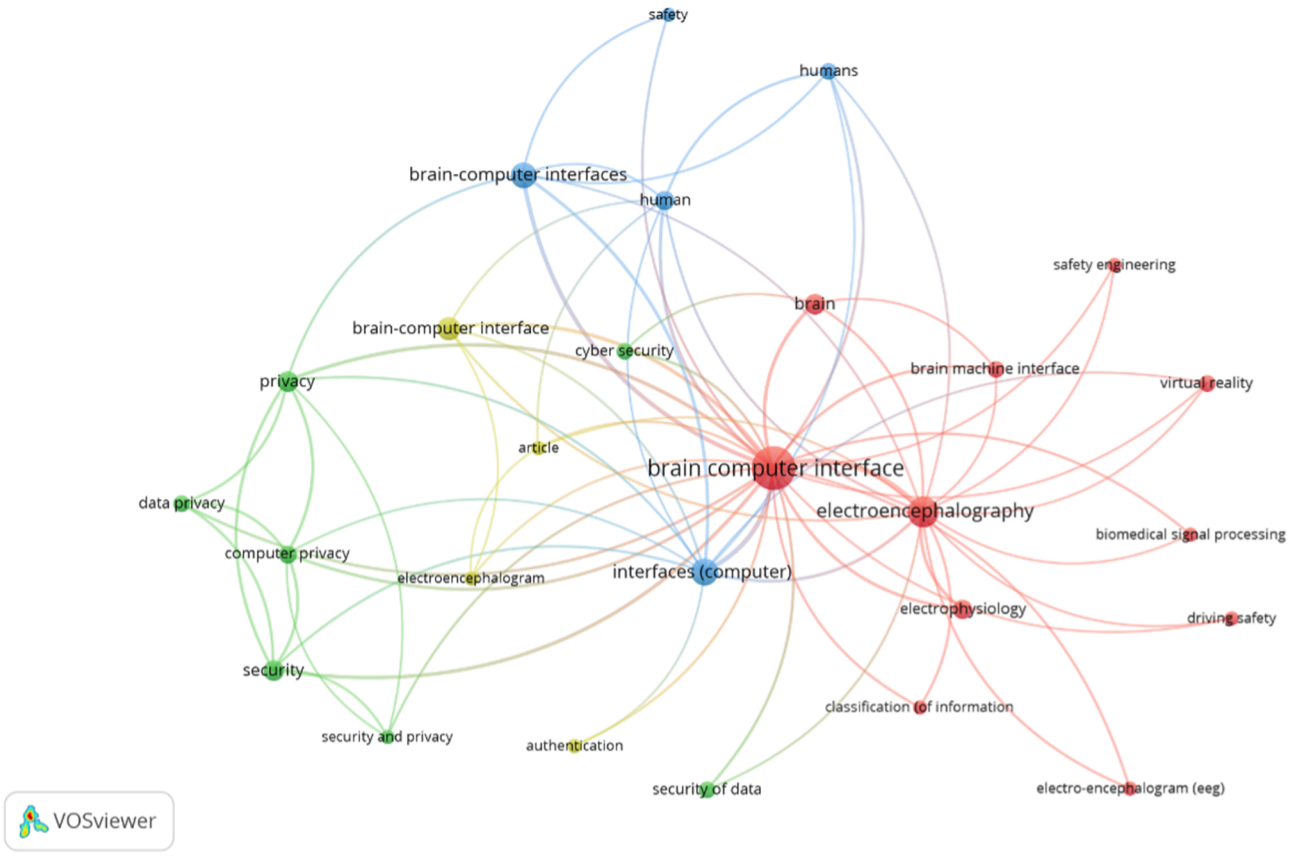

Fig. 4. Visualization of all keywords with the VOSviewer software (Scopus Database) (Vosviewer, 2022).

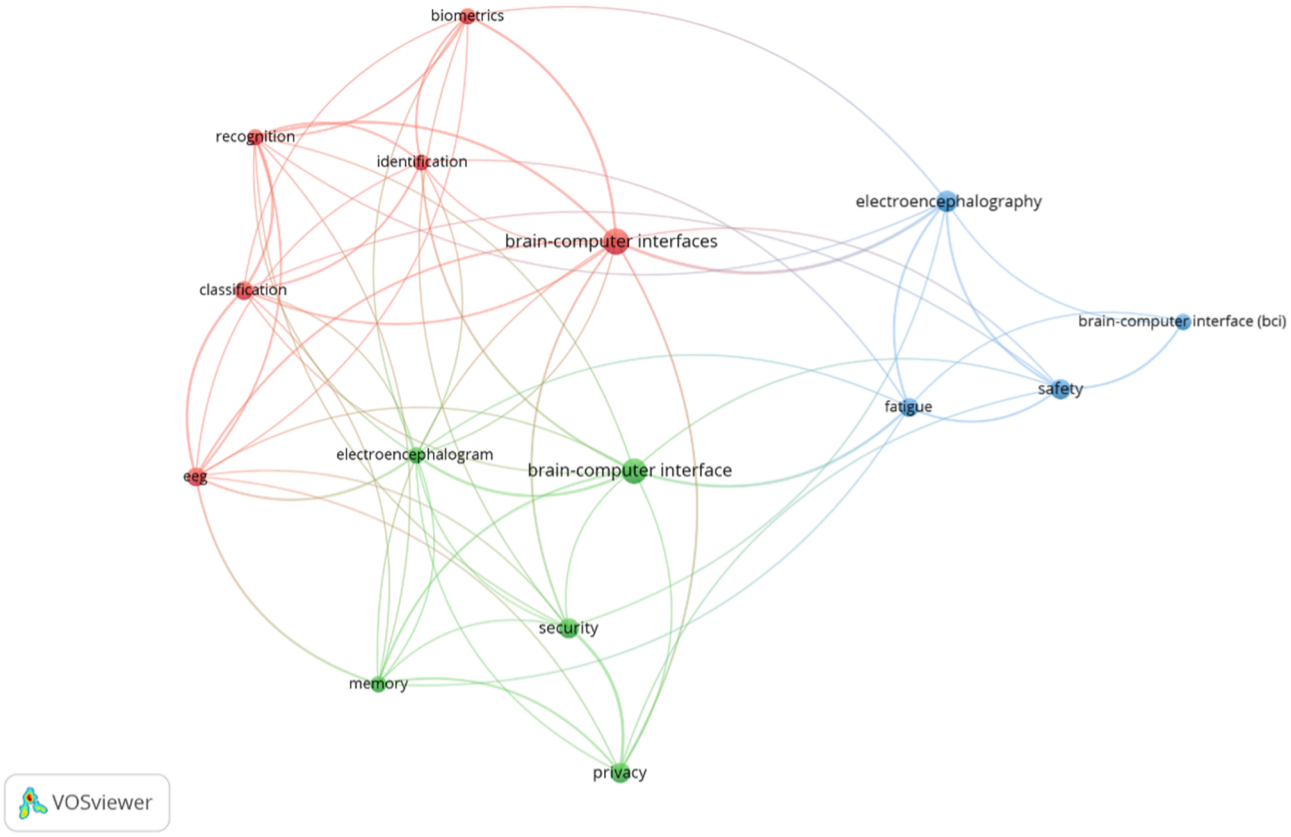

Fig. 5. Visualization of all keywords with the VOSviewer software (WOS Database) (Vosviewer, 2022).

Table 4
Classification of results according to thematic categories.

Safety			Security	
Risk identification	Fatigue detection	Safety control	Cyberattacks	Authentication
7	10	6	17	8
23			25	

Table 5
Classification of the results according to the search strings 1–4.

	Search string 1	Search string 2	Search string 3	Search string 4
	Safety or Security	Safety	Security	Security and Safety
Results	48	26	22	3

narrative description of thematic categories of safety and security fields. The analysis of the BCIs as an emerging risk is configured by the type, level, and strategies for emerging risk management. Such structure is shown schematically in Fig. 3.

3.1. Bibliometric characteristics

The bibliometric characteristics of the 48 results presented in Appendix Table A1 are shown. These characteristics are organized around research areas, keywords, fields, and categories.

3.1.1. Research areas

Considering the 48 results shown in Appendix Table A1, 31 are articles (65 %), 14 are proceedings papers (29 %) and 3 are book chapters (6 %). Regarding the research areas, the percentages found are approximately (% of 48 articles): computer science (76 % results), engineering (70 % results), Mathematical Computational/Biology (52 %), Neurosciences/Neurology (50 %), Radiology Nuclear/Medicine Medical/Imaging (39 %) and Communication (32 %) stand out. Other areas have lower results (<20 %), particularly telecommunications (16 %), and mathematics (14 %). The other areas have more residual results (<10 %). Said results are shown in Table 2 distributed by year of publication.

3.1.2. Keywords

A co-occurrence analysis for the WOS and Scopus databases has been made with the VOSviewer software. In both cases, all keywords and full-count options were used. The minimum number of occurrences of a set of keywords was 4, and 4 clusters with Scopus and 3 clusters with WOS were found. The keywords and the number of occurrences are presented in Table 3 and the clusters are shown in Fig. 4 and Fig. 5 based on the most frequent keywords.

3.1.3. Fields and categories

The 48 results are shown in Table 4 according to the fields of study and thematic categories defined in the methodology. Thus, 23 results are grouped within the safety field and 25 within the security field, representing 48 and 52 %, respectively. The categories with the highest results are fatigue detection and cyberattacks in these fields, with 10 and 17 results, respectively.

Table 5 shows the results obtained within the field “safety” or “security” or “security and safety” applying the search strings. When these results are compared with those of Table 4, it can be observed: Search string 1: the 48 results are the same as those shown in Table 4; Search string 2: of the 26 results, 23 are included within the safety field, and 3 are included within security (Belkacem & IEEE, 2020; Bernal et al., 2021; Bernal, Sergio López et al., 2022); Search string 3: the 22 results are within the 25 of the security field; Search string 4: 3 results that are within security and safety (Karim et al., 2019; Kim et al., 2021; Sciaraffa et al., 2020).

3.2. Thematic categories for safety field

The results of the safety field are shown below. Such results are composed of risk identification, fatigue detection, and safety control categories.

3.2.1. Risk identification

Different works based on the application of non-invasive BCIs have been identified under this category to identify risks of occupational accidents and evaluate and train certain cognitive and physiological conditions linked to the prevention of occupational accidents. In addition, in the context of informed consent in implantable BCI research, two studies have been identified that analyze a broad set of BCI risks.

About the application of non-invasive BCIs in the occupational context, 5 works have been identified. Regarding the risk identification process, Lee & Yoo (2012) developed a cognitive assessment tool based on BCI to prevent users from unexpected safety-accident. This approach is different from those studies based on assessing the cognitive status through EEG signal. Sciaraffa et al. (2020) differentiate between traditional BCI and passive BCI, indicating that the basis of traditional BCI systems is the “overt” detection of human intention, while in the case of passive BCI, it is the “covert“ monitoring of real human mental states. According to this author, the development of these passive BCIs is driven by safety–critical applications since it improves the so-called human–machine interaction (HMI). Zhou et al (2021) made a laboratory experiment that recorded the hemodynamic responses with near-infrared spectroscopy (NIRS)-based BCI (non-invasive method). This experiment was identified salient prefrontal cortex (PFC) areas that signify different construction risks, showing that the left PFC was more engaged in risks recognition; in particular, the dorsolateral PFC was identified for electricity and impact-related recognition risks and the ventrolateral PFC for stabbing-related recognition risks. These results sing out the potential of NIRS-based BCIs for hazard inspections.

Regarding the evaluation and training of specific cognitive and physiological conditions, Kim et al. (2021) present the development of an information security-enforced EEG-based classification system for evaluating nuclear power plant operators and determining their fitness for duty for safe nuclear reactor operations. Huang et al. (2021) propose a virtual reality system for construction safety training, based on BCI and physiology data, which facilitates understanding workers’ physical condition, enhancing safety awareness, and reducing accidents. Regarding improving the efficiency of safety training, Zhou et al. (2021) indicate that a BCI can be used to provide real-time hazard recognition performance feedback and thus improve demonstration strategies.

In the context of informed consent in implantable BCI research, Klein (2016) proposed six core risk domains relevant: short and long-term safety, cognitive and communicative impairment, inappropriate expectations, involuntariness, affective impairment, and privacy and security. Additionally, identity, agency, and stigma are identified as non-traditional risks. Similarly, Klein & Ojemann (2016) consider several BCI research risks, including safety concerns, cognitive and communicative impairments, inappropriate subject expectations, group vulnerabilities, privacy and security, and disruptions of identity. Regarding safety concerns, these authors consider associated risks to the component implantable BCI. The components of implantable BCI are recording and stimulating electrodes, power generation and delivery, and data processing and transfer. Regarding the safety risks are grouped into three principal types: implantation, biocompatibility, and longevity.

3.2.2. Fatigue detection

The number of works that address the study of mental fatigue through BCIs stands out. Thus, the study of mental fatigue applied to driving safety has been addressed by various authors (Liu et al., 2015;

Liu et al., 2016; Min & Cai, 2020; Ming et al., 2021; Zhang, Z. T. et al., 2016). Moreover, the study of cognitive states induced by mental fatigue has been applied to aircraft pilots (Han et al., 2019) and high-speed train drivers (Zhang, X. L. et al., 2017). Similarly, Deahais et al. (2018) measure neural correlates aircraft pilots' working memory performance in real flight conditions.

The study of mental fatigue through BCIs also has been applied in other activities different from driving or piloting. For example, Tsai (2017b) proposes an approach for studying the mental fatigue of workers of nuclear power plants by monitoring their brain wave rhythms through a BCI, and Tsai (2017a) proposes other approach based on physiological status monitoring of construction workers based in BCI to analyze fatigue levels.

3.2.3. Safety control

The applications identified on safety control are mainly related to robotization. Thus, have been identified applications on prostheses, exoskeletons, and collaborative occupational environments between robots and workers.

About applications on prostheses, Wester et al. (2013) present an experimental validation of software-based safety features implemented during the control of a prosthetic limb in self-feeding tasks with a quadriplegic patient using implanted intracortical electrodes. Regarding applications on exoskeletons, Witkowski (2014) proposed a novel hybrid brain-neural computer interaction (BNCI) system fusing EEG and electrooculography (EOG) to enhance the reliability and safety of continuous hand exoskeleton-driven grasping motions.

Considering the collaboration and coincidence, both spatial and functional, between workers and collaborative robot systems and semi-automated machines, Neu et al. (2019) propose a theoretical approach to occupational cognitive protection in HMI scenarios to detect and prevent accident causes such as stress, fatigue, and inattention. Penaloza et al. (2015) present an approach using EEG signals, detecting a brain potential called error-related negativity (ERN) that spontaneously occurs when the operator perceives an error made by the robot or when an unexpected event occurs. This signal sends an emergency stop of a robot when the human operator perceives such an error or unexpected event. Li et al. (2020) developed a robust nonlinear predictive controller based on sliding mode for brain-controlled mobile robots with the main goal of incorporating and improving the safety and robustness of BCI-based real-time control.

Considering the difficulty of collecting labeled EEG samples concerning unlabeled samples that can be abundant in real applications, both used in EEG-based BCI, She et al. (2020) propose an algorithm to evaluate the risk of these unlabeled data by a new safety control mechanism.

3.3. Thematic categories for security field

The results of the security field are shown below. Such results are composed of cyberattacks and biometric authentication categories.

3.3.1. Cyberattacks

The transfer of BCI technology from the laboratory to real-world presents challenges regarding confidentiality, integrity, and availability of universal access systems (Bahr et al., 2011). The BCIs that record EEGs, and the abuse of procedures or data can directly affect the person whose EEG is recorded (Landau et al., 2020). For example, Pittman et al. (2018) describe the implementation of cybersecurity controls in support of curating research data in a new brain-machine interface laboratory.

Belkacem (2020) describes a cybersecurity framework that consists of risk scenarios and provides solutions for privacy and security issues related to P300-based BCI applications because it is the most popular modality. Bonaci et al. (2015) indicate that the methods to prevent security and privacy threats arising BCIs should be developed in the early design phase and integrated throughout the TLC and from an interdisciplinary perspective. Regarding the BCI life cycle, (Bernal et al., 2021) present a new version of the BCI cycle, defined as a closed-loop process with five phases to homogenize the BCI cycle to include neural data acquisition and stimulation processes. These phases are: (1) Brain signals generation; (2) Neural data acquisition & simulation; (3) Data processing & conversion; (4) Decoding & encoding; (5) Applications. These authors analyze for each phase the security mainly from a technological point of view. For it, these authors define tasks, inputs, and outputs and analyze the attacks affecting the devices implementing each phase and their impacts and countermeasures.

Through these cyberattacks, emerging two specific concerns. Firstly, the user's private information could be obtained without their consent, and secondly, the behavior user could be altered by acting on neural activity.

Regarding the first concern, Lange et al. (2018) have obtained experimental results suggesting that the extraction of specific PIN codes from EEG signals is theoretically feasible for some users and PINs. These experiments indicate that privacy concerns may be more important than security concerns in BCI-based applications. Karim et al. (2019) address the study of Bluetooth operating parameters necessary to meet the performance, usability, and privacy requirements of reliable and secure mobile BCIs applications. To avoid the alteration or attack of the EEG signal during the transmission of the wireless BCI, Bhalerao et al. (2020) introduce a security lock-in between the EEG recording system and the processing system.

Bellman et al. (2018) studied as attackers can obtain private information from individuals without their consent using modern consumer-grade BCI devices based on the level of recognition a victim has of a specific face. For example, Gladden (2016) proposed a conceptual framework neuroprosthetic devices (sensory, cognitive, and motor neuroprostheses), utilized for the treatment of medical conditions or purposes of human enhancement. The aim of such a framework can aid in exploring the practical, legal, and ethical issues that arise because these devices have the technological potential that, in the future, could be used for the two critical functions of neuromarketing related to the collection of data on the cognitive activity of the device's human host or influence host behavior. In this way, Lange et al. (2018) consider that it is quite possible to design malicious applications with which, for example, EEG signals collected for gamming, can be used to reveal other types of correlations, such as medical or political. On the internet of health things context, Xia & Fan (2020) studied the construction of sports injury rehabilitation systems, based on motor imaging BCI, where maintained security and privacy of this medical system.

Regarding the second concern, considering a future possibility of influencing or alternating human behavior, Moioli et al. (2021) have studied an interdisciplinary research field resulting from the intersection of neurosciences and wireless communications (as well as signal processing, control theory, and computer science), whose applicative encounter could occur with developments in future wireless networks 6G, which will support BTC and will generate great dilemmas in security, privacy, and ethics. These authors propose a very interesting hypothesis based on the that with current BCIs it is possible to influence human behavior by directly modulating the brain in clinical settings, the future BCIs in a wireless network context could receive read and write signals unwanted, not necessarily malicious, that could have the potential to interact with behavior, thus being able to influence both individually and socially. Morales et al. (2009) proposed a networked biosystem secure, reliable, and scalable in this network context.

Bernal et al. (2020) have analyzed the security and privacy vulnerabilities in emerging neurostimulation technologies implemented through micron-scale BCI. For this, these authors have experimentally simulated two types of neuronal cyberattacks that affect the biological activity of neurons. These cyberattacks are called Neuronal Flooding (FLO) and Neuronal Scanning (SCA). Among the main results of these experiments, it stands out that both types of cyberattacks are adequate to affect neuronal activity, with FLO being more effective in immediate

Table 6
Search strings 1 and 5 to compare security, safety, and risk results.

Database	Year 20XX	09	10	11	12	13	14	15	16	17	18	19	20	21	n
Scopus	Search string 1	1	0	1	1	3	6	5	4	4	8	6	8	6	40
	Search string 5	1	0	0	0	1	3	1	0	0	1	1	3	1	12
WOS	Search string 1	0	0	1	1	1	1	3	7	6	2	5	7	6	40
	Search string 5	1	0	0	0	1	3	1	0	0	1	2	1	1	11

terms and SCA in the long term. In a similar simulation experiment, (Bernal et al., 2022) presented the Neuronal Jamming (JAM) cyberattack, which aims to inhibit neuronal activity. The JAM cyberattack was analyzed on biological and artificial scenarios, as well as compared to FLO.

3.3.2. *Biometric authentication*

New techniques are emerging based on non-invasive measurements to overcome the limitations of traditional authentication systems (Chen et al., 2016). In this regard, artificial biometrics is a powerful security research tool that generally includes the recognition of a person's identity from the biometric data collected, including, among other, physiological characteristics which can be collected visually or through some specialized devices (Sourin et al., 2016). Thus, the use of EEG signals as a unique biometric trait of every-one (these signals carry genetic and individual information) promotes the development of new applications based on BCI as a more robust security system than traditional security mechanisms such as PINs, ID cards, passwords, etc. (Kaur et al., 2020). Moreno-Rodriguez et al. (2021) introduce an open-access database of synchronously recorded EEG signals, voice signals, and video captured for biometric purposes. This approach applies to unimodal biometric systems, especially for evaluating multimodal variants in the BCI and faces recognition projects.

In this way, the EEG is the most viable technology for biometric authentication applications due to the ease of use, portability, relatively low cost, and high temporal resolution (Chen et al., 2016). In this regard, three examples are shown next. Narayana et al. (2019) present an important application for the physically challenged consisting of a biometric security system configured by a BCI to lock/unlock a wheelchair and control its movements using these patterns that occur due to eye blinks and activity of muscles in the jaw. Alomari et al. (2017) propose that a practical EEG-based system could be developed to make it easier for users to select a password based on the prediction of its memorization at the time of its creation. Merrill (2019) designed a brain-based authentication system using custom-fit EEG earpieces.

Nevertheless, the resolution and reliability of EEG information is still limited (Yang, 2019). Chen et al. (2016) compared the wet and dry electrodes as authentication systems. They concluded that the dry ones show sufficient precision for high-security applications, allowing commercialization and highlighting their practicality. However, Kaur et al. (2020) consider that EEG device technologies with dry electrodes need to be tested for their suitability as biometric applications. So, such authors sing out the following key points that need to be discussed while building EEG-based security: emotions impact on neuro signals, permanence factor of neuro signals (age variation), EEG acquisition tools complexity, and development of multimodal systems.

3.4. *BCIs as an emerging risk.*

The analysis of the BCI as emerging risk is carried out under the scenario "general – general" established by Brocal et al. (2021) and consists of applying the following three steps, as described in the method section (the terms BCI and BCIs are used interchangeably and with their general meaning). Firstly, the type of emerging risk (ERi) is defined using the models proposed by Brocal et al. (2017; 2018). Secondly, the level of emerging risk is determined through the emerging risk classification scheme proposed by Brocal et al. (2021). Thirdly, the strategies for emerging risk management are defined through the criteria also established by Brocal et al. (2021).

3.4.1. *Type of emerging risk*

With the evolution of the number of results analyzed through the search strings used, in Table 2, it is observed that the first work was published in 2009, and between that year and 2014, only one result was published annually (except 2010, where no paper was published). Although, as of 2015, the number of papers published annually increases, the upward slope is still very smooth, with a maximum of 10 works published in 2020. Such circumstances allow to point out the initial moment (2009) of this exploration approach and its still germinal phase. This germinal phase coincides with the embryonic phase defined

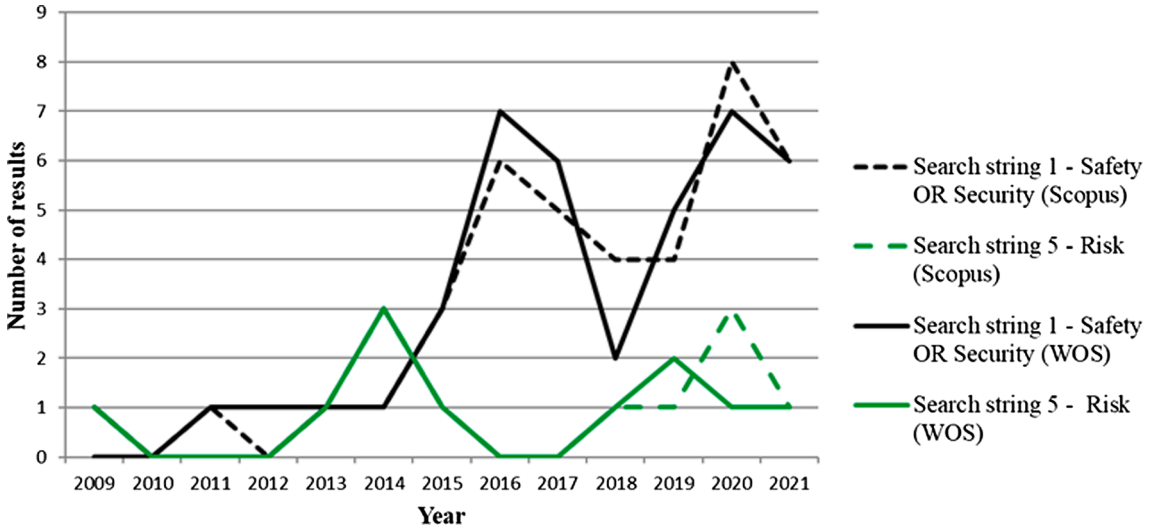

Fig. 6. Search strings 1 and 5 to compare security, safety, and risk results.

by Brocal et al. (2017; 2021; 2018).

Complementarily, in Table 6 and Fig. 6, the results of search string 1 are compared with search string 5 that is shown below:

Scopus database: (AUTHKEY ("brain-machine interfaces") OR AUTHKEY ("brain-computer interfaces")) AND (AUTHKEY ("risk"))

WOS database: ((AK= ("brain–machine interface")) OR AK= ("brain–computer interface*")) AND (AK=("risk*"))*

The germinal phase mentioned above can be verified, in the context of the risk associated with BCI, with the results of the Table 6 and Fig. 6.

The BCI is a clear example of an emerging risk that is new due to the following reasons linked to the conditions (Ci) modeled by Brocal et al. (2017; 2021; 2018). Firstly, this device complies with condition C1 because this risk did not previously exist and is caused by one new technology. About it, Denning et al. (2009a) concluded in 2009 that the security challenges of BCI technology would likely be very different from those of traditional computer security. Therefore Landau et al. (2020) consider the BCI as a relatively new domain that generates new problems that must be addressed before the use of this technology is more widespread. This relativity can be interpreted considering that BCI research began in 1973 (Landau et al., 2020), although it is in recent years when that is of increasing interest to researchers (Burwell et al., 2017; Landau et al., 2020; Li et al., 2015; Ramsey, 2020). Considering, for example, for the security field, Bernal et al. (2021) determined that the BCIs are in an early and immature phase because the scientific literature has not addressed this critical area until recent years. In this regard, it is essential to indicate that the development of this field, especially the cyberattacks category is more advanced than the other categories analyzed here. Therefore, it can infer that for both fields, safety and security, the set of categories is not mature. Secondly, although the risk seems to be increasing, according to condition C4 (number of hazards leading to the risk is growing), it is too early to state that the risk increases according to the growth phase defined by Brocal et al. (2017; 2021; 2018).

3.4.2. Level of emerging risk

Applying the approach proposed by Brocal et al. (2021), the level of emerging risk is a function of its uncertainty (Q) and its potential consequences (C). Regarding Q is a function of the quality of knowledge (K) and the level of understanding (N) about the emerging risk.

In this way, the level of knowledge (K) is low considering the number, evolution, and characteristics of the results analyzed in this work. In addition, the BCI also needs the development of specific legislation and standardization. In this way, various authors (Belkacem & IEEE, 2020; Bernal et al., 2020; Moioli et al., 2021) point out the need to advance in the regulation and standardization of BCIs and their security problems.

Regarding the level of understanding (N) of the interaction of the BCI with the brain is also low. For example, Bernal et al. (2022) consider it essential to understand the relationship between brain disorders and brain connectivity. Moreover, the long-term effects of BCIs on psychology, neurophysiology are unknown. In 2009 Denning et al. (2009b) concluded that neural changes made by hackers through these devices could have irreversible effects on human performance and cognition. About, Bernal et al. (2021) consider that research papers that analyze the impact of cyberattacks on neuronal activity do not usually study physiological or psychological effects.

Thus, with the combination of the qualitative results of K (low), and N (low) the degree of uncertainty (Q) is high.

Regarding potential consequences (C), considering the categories indicated by Brocal et al. (2021) should be considered high. The reasons for this categorization are as follows. The losses and damages are difficult to specify, especially considering the previous combination of the qualitative results of K (low) and N (low). In addition, these consequences have the following potential characteristics described by Kristensena et al. (2006): reversibility, persistence, ubiquity, and delay effects. The main common denominator known for these characteristics is cyberattacks. Thus, reversibility and persistence are related to the potential irreversible effects on human performance and cognition. Ubiquity is due to the geographical dispersion of potential damage through cyberattacks. And delay effects also are related to cyberattacks and the fact that the long-term effects of BCIs on psychology, neurophysiology are unknown.

Consequently, with the combination of the qualitative results of Q (high) and C (high), the level of emerging risk is high.

3.4.3. Strategies for emerging risk management

Due to the previous results, this emerging risk can be considered an ER1, so the three RMSi considered by Brocal et al. (2021) could, in theory, be compatible with this risk.

The combined application of the three strategies is complex. In any case, the result of this combination should include an approach based on the precautionary principle that includes the definition of risk treatment measures and measures to build confidence and trustworthiness. Risk treatment measures should be defined in the form of avoidance, reduction, transfer, and retention. As for the measures to build confidence and trustworthiness, they should pursue the reduction of uncertainties, clarification of facts, involvement of the people affected, deliberation, and accountability.

4. Discussion

The method used has made it possible to obtain a set of results to explore the trends and main research needs on the risks and applications of BCIs in the safety and security fields. Said results are analyzed below using the structure used in the previous sections to facilitate the reading and correspondence between these results and their discussion.

4.1. Bibliometric characteristics

A total of 48 results, distributed mainly between 29 % of proceedings and conference papers and 65 % of articles, have been obtained based on search string 1 and the established inclusion and exclusion criteria.

This combination of results limits the quality of the analyzed works, although, in return, it allows broadening the perspective of bibliographic exploration, the main objective of this research. Similarly, not limiting the search time interval allows observing the evolution of the number of works. Such circumstances allow to point out in 2009 the initial moment of this exploration approach and its still embryonic phase.

Such evolutionary characteristics coincide with the growing interest of researchers in BCI technologies, as expressed by other authors (Burwell et al., 2017; Li et al., 2015; Ramsey, 2020) and especially with Landau et al. (2020).

An optional consultation stage in conducting the scoping study could be added to improve these results, as proposed by Arksey & O'Malley (2005). On the other hand, the number of results could increase with other search strings that include different keywords and other field tags. A systematic literature review could also be considered. Said modifications in the literature review method could have the advantage of including a more significant number of studies focused on specific risks of the BCI, for example, according to the categories studied in this study or others such as focused on ethical or legal aspects discussed in the scoping review of Burwell et al. (2017). And as a drawback, the exploration perspective shown here could be reduced.

4.1.1. Research areas

Regarding the research areas covered by the set of results obtained, the broad multidisciplinary nature of the study of the risks and applications of BCI in the fields of safety and security is evident. Areas stand out in computer science (76 %) and engineering (70 %) versus Neurosciences/Neurology (50 %) and Radiology Nuclear/Medicine Medical/Imaging (39 %).

This multidisciplinary context coincides with that shown by Wester

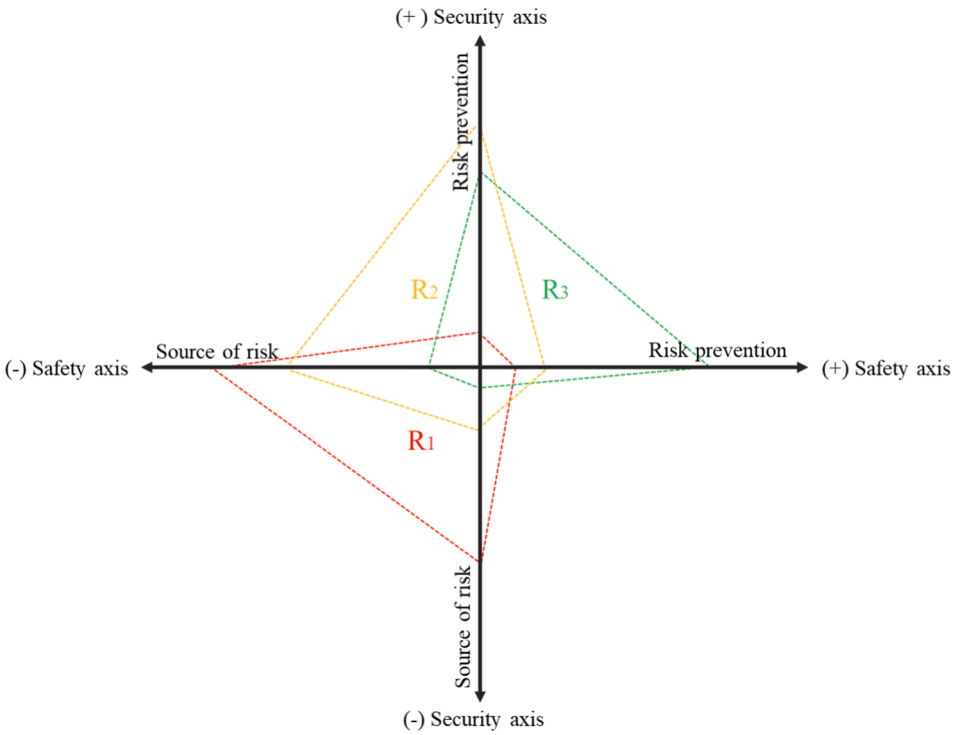

Fig. 7. BCI risk configuration as the quadrilateral area defined by the safety and security axes.

et al. (2013) whose consider that BCI context involves technological advancements and collaborations in robotics, neuroscience, computer science, materials science, and signal processing.

However, this multidisciplinary approach is not observed in a generalized way on the individual works analyzed, especially under collaboration between engineering and/or medical and/or neuroscience areas or departments.

4.1.2. Keywords

The number of keywords in the Scopus database is approximately double that of the WOS database. Thus of the 625 keywords in Scopus 27 meet the threshold. And in WOS of the 291 keywords 15 meet the threshold.

There are three alternative denominations in both databases for the term BCI. Thus, in Scopus, the corresponding keywords are: brain computer interface (35 occurrences), brain-computer interfaces (12), and brain-computer interface (10). And in WOS: brain-computer interfaces (10), brain-computer interface (9), and brain computer interface (bci) (4).

For the keywords safety and security, the number of occurrences does not stand out in general over the other keywords, except mainly for the keywords related to BCI.

Regarding the formation of clusters, in the case of the Scopus database, it stands out (Fig. 4): keywords such as driving safety and safety engineering are part of cluster 1 (11 items, red). The keyword security is part of cluster 2 (7 items, green), linked mainly to privacy-related keywords (data privacy, security and privacy, and computer privacy). The keyword safety is part of cluster 3 (5 items, blue), mainly linked to the keyword humans. And in the case of the WOS database (Fig. 5): the keyword security is part of cluster 2 (5 items, green), linked to keywords such as privacy. And the keyword safety is part of cluster 3 (5 items, blue), related to keywords such as fatigue.

4.1.3. Fields and categories

Concerning the safety and security risk fields studied, there is a correspondence of 88 % when the results of Table 4 and Table 5 are compared. This shows a good correspondence between the classification criteria of the safety and security fields (based on the work of (Peter Blokland & Genserik Reniers, 2017) and the search strings used.

Such correspondence can also be seen with the cluster analysis results in the previous section. For example, the keyword safety is linked to categories like fatigue. And security is linked to keywords related to privacy.

The five thematic categories defined allow defining a general risk framework related to BCI's safety and security. Regarding the categories that stand out for their number of studies are fatigue detection and cyberattacks for the safety and security fields, respectively. In the case of the cyberattacks category, it should be noted that its number of results is rough twice that of the other categories.

4.2. Thematic categories

Two clear research trends can be observed in safety and security fields. These two trends evolve on the concepts of the source of risk and technology for risk prevention. This differentiation suggests the existence of two poles of opposite signs or two axes on the BCI technology. On the one hand, the BCI is studied as a source of risk, that is, as the origin of potential harm to the user of an unintentional (safety) or intentional (security) nature. On the other hand, the BCI is studied as a technology for risk prevention, that is, as a measure to avoid or minimize, failing that, potential harm to the user of an unintentional (safety) or intentional (security) nature.

This approach allows the conceptual configuration shown in Fig. 7. In this way, the BCI risk can be represented by the quadrilateral area defined by the four values of the variables considered. Fig. 7 shows three examples categorized from higher risk (R1) to lower risk (*R*3).

This approach can be modeled both qualitatively and quantitatively. As an idea, a relatively simple approach that would allow representing the quadrilateral area of a given BCI Risk, could be based on the design of appropriate scales, for example, through the Delphi method, using the Likert 5-point scale. In this way, it would be possible to assign numerical values to each of the four variables considered for said BCI Risk, these variables being: (i) Source of risk (- safety axis); (ii) Risk prevention (+safety axis); (iii) Source of risk (- security axis); (iv) Risk prevention (+security axis).

In any case, the development of such an approach is beyond the objectives of this research, although it indicates a clear line of future research. In such modeling, the uncertainty variable could be integrated as a third dimension or third axis to analyze risk as an emerging risk.

4.2.1. Safety field

In this safety field, two groups of works can be differentiated, depending on whether they are based on the application of non-invasive or invasive BCIs. The three categories (risk identification, fatigue detection, and safety control) are mainly based on non-invasive BCIs, especially with EEG technology. Regarding the works based on invasive BCI, the works of Kein (2016) and Klein & Ojemann (2016) classified in the risk identification category stand out.

The works based on non-invasive BCIs are characterized by the application of the BCI as a technology for risk prevention, mainly of an occupational nature. On the other hand, regarding the work based on implantable, BCI research is characterized by considering BCI as a source of risk.

4.2.2. Security field

In this security field, the same two groups of works identified for the safety field can be identified, that is, non-invasive and invasive BCIs. Likewise, the two categories analyzed are mainly based on non-invasive BCIs, especially with EEG technology.

Regarding the approach of the cyberattacks category, it is characterized by addressing the BCIs in a broader way than the other categories analyzed for the following reasons. First, the study of risk is proposed as an integrated approach throughout the TLC and the BCI cycle. Second, this approach allows each phase of the BCI cycle to be analyzed under the dual consideration of its quality as a source of risk and technology for risk prevention. Finally, regarding the different risks addressed from this category, the possibility of altering neural activity through these BCI devices should be pointed out due to their unique importance.

Regarding the biometric authentication category, it can be considered a technological preventive measure to improve the security process in authentication activities.

4.3. Other fields and categories

The fields of study and thematic categories defined with this research are not a taxonomy but rather an exploratory approach that allows determining the first step towards more specific studies on the risks and applications of BCI in safety and security fields, among them that taxonomy that could be developed. For example, Landau et al. (2020) present an interesting taxonomy of the current trends in BCI systems based on EEG and its domains linked to the security and privacy field. Such taxonomy has this structure: security (authentication, cryptography, lie detection), medical (diagnosis), and entertainment (gaming). Another example is presented by Bernal (2021), and it consists of two main attacks on brain categories during neurostimulation. A category consists of taking control of the stimulation process to cause neural tissue damage. The other category focuses on inducing an effect or perception in the user. In this way, it should be noted that with the results of this work, a similar investigation in the field of safety has not been identified.

Thus, the need for future research that deepens the definition of the key terms related to the safety and security of BCIs is evident. In this regard, some specific terms have been identified during the bibliographic analysis process. Among these terms, the following stand out: exocortex (Bonaci et al., 2015), neuroergonomics (Dehais et al., 2018), neurosecurity (Bernal et al., 2021; Bernal et al., 2022; Bonaci et al., 2015; Klein, 2016), neuroethics (Belkacem & IEEE, 2020; Bernal et al., 2021; Klein, 2016; Klein & Ojemann, 2016).

As additional part of the results of this exploratory approach, the results of a search for these terms in "all fields" and without restrictions in the WOS and Scopus databases are the following: exocortex: 6 and 47; neuroergonomics: 679 and 2053; neurosecurity:10 and 8; neuroethics: 1439 and 7562.

Given the exploratory characteristics indicated above, a detailed analysis of the previous terms will not be carried out here, only an approximation as follows. Thus, considering the previous results, as well as the definition of neuroergonomics according to Parasuraman (2003) and neuroethics according to Marcus (2002), it is evident that these fields are more developed than those related to exocortex and neurosecurity, probably because their field of application it goes beyond BCIs.

Regarding exocortex and neurosecurity definitions, Bonaci et al. (2015) indicate that the term exocortex stems from computer science and evolutionary psychology, and it is defined as "a wearable (or implanted) computer used to augment a brain's biological high-level cognitive processes and inform a user's decisions and actions". Also, Bonaci et al. (2015) indicate that Denning et al. (2009) introduced the term neurosecurity as "protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will". Thus, the definition of the term exocortex is technological and related to the general operation of the device. The definition of the term neurosecurity is preventive and related to device-specific security from malicious parties.

In principle, the concept of security analyzed in this research includes the concept of neurosecurity. The same is not the case with the concept of safety. Therefore, the use of the term "neurosafety" seems logical as an additional and complementary component. However, in the publications analyzed, this term has not been identified. With the further search for "neurosafety" in "all fields" and without restrictions in the WOS and Scopus databases, 6 and 5 results were obtained, respectively. And with the analysis of these results, the definition of the term neurosafety is not identified either. However, the term is used in research areas related to neuroscience, physiology, and pharmacology. It follows that said term is restricted to said research areas.

The need seems to emerge from all the above for a new area of specific research on safety and security for BCIs. Such need implies a more precise determination of related study intervals. For it and as an initial approach, the first level of this area could be called "BCIs risks" which would have a general scope. Then, the said level could descend towards more specific levels, for example, under the names "BCI security" and "BCI safety.".

Thus, considering the set of results and analysis carried out with the present investigation, the following definitions can be proposed:

- *BCI security: The study of BCIs as a source of risk and a measure to prevent direct, indirect, and induced damage to users' health and their environment of intentional origin.*
- *BCI safety: The study of BCIs as a source of risk and a measure to prevent direct, indirect, and induced damage to users' health and their environment of unintentional origin.*

The concept of "damage" in the previous definitions must be understood in a broad sense both in terms of time, the short and long term, as well as health. And for health, the definition of the WHO is adopted (World Health Organization, 2020): "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity.".

In any case, the proposed definitions are a first step towards differentiating the two study intervals considered for the BCIs.

4.4. BCIs as an emerging risk

The results obtained from the analysis of the BCI as an emerging risk are mainly limited by three interrelated factors, being: (a) the qualitative characteristics of the theoretical framework proposed by Brocal et al. (2017; 2021; 2018); (b) the bibliographic review method used; and (c) the generic characteristics of the BCIs technology that have been considered.

Thus, the qualitative results of the type of emerging risk, level of emerging risk, and the strategies for emerging risk management can be considered a general risk framing or general pre-assessment of the BCI technology. These results could be improved with modifications in the bibliographic review method and curves other than the TLC on the S-curve. For example, the analysis of the consequences could be extended by considering categories other than cyberattacks. In addition, among other modifications, the study of data and specific BCI technologies could be considered (for example, between non-invasive or invasive technologies, there could be significant differences). With all this, more detailed results could be obtained, especially concerning the behavior of uncertainty (Q.).

In any case, it is not foreseeable to obtain results other than the classification of the BCI as an emerging risk that is new or, failing that, as an emerging risk that is both new and increasing. This assertion is mainly because the BCIs are immature or embryonic from a risk, safety, and security perspective.

5. Conclusions

The conclusions are presented below, taking the objectives established as the guiding thread.

Thus, regarding to the general objective, the trends and main research needs on the risks and applications of BCIs in safety and security are as follows:

1. ***The research areas involved are highly multi-disciplinary***. Computer science and engineering areas sing out on Neurosciences/Neurology and Radiology Nuclear/Medicine Medical/Imaging.
2. ***BCIs are studied under a dualistic approach to risk, both as a source of risk and as a technology for risk prevention.*** This differentiation suggests the existence of two axes on the BCI technology. On the one hand, the BCI is studied as a source of risk of an unintentional (safety) or intentional (security) nature. On the other hand, the BCI is studied as a technology for risk prevention, that is, as a measure to avoid or minimize, failing that, potential harm to the user of an unintentional (safety) or intentional (security) nature.

   Considering the structure configured by said axes, according to Fig. 7, a summary of the risks and applications obtained with the present research would be:

   (i) Source of risk (- safety axis): When a source of risk is of an unintentional (safety) nature, it highlights the possibility of consequences related to the health of the user (for example, of a physiological or cognitive nature), as well as to variables in their technological environment (for example, involuntary actions on control systems).

   (ii) Risk prevention (+safety axis): When technology for risk prevention is unintentional (safety), for the "risk identification" category, worth mentioning applications related to safety inspection tasks, unexpected accident prevention, activities in hazardous facilities, and training systems based on virtual reality. Furthermore, for the "fatigue detection" category, the applications are related to the study of mental fatigue applied to driving safety, aircraft pilots, and high-speed train drivers, as well as other activities different from driving or piloting, for example, the fatigue of workers of nuclear power plants or construction workers. Finally, regarding the "safety control" category, applications on prostheses, exoskeletons, and collaborative occupational environments between robots and workers stand out, as well as occupational cognitive protection in HMI scenarios to detect and prevent accident causes such as stress, fatigue, and inattention.

   (iii) Source of risk (- security axis): When a source of risk is of an intentional (security) nature, it highlights the possibility of losing the user's private information and modifying their behavior by altering their neural activity.

   (iv) Risk prevention (+security axis): When technology for risk prevention is of an intentional (security) nature, the "cyberattacks" and "biometric authentication" categories are self-explanatory about their fields of application.
3. ***Research is still in an early phase.*** The characteristics of works found in the databases and the thematic categories identified show an early phase that sings out two trends. First, the specific terms are evolving, for instance, neurosecurity and neurosafety. However, these terms are not mature, nor do they adequately reflect the scope described in the present research. Therefore, three new terms have been proposed as an initial approach: "BCIs risks," which would have a general scope. And "BCI security" and "BCI safety" have a more specific scope. Second, the scope of the analyzed works on the relationship between the technology of humans and industrial safety is significantly scarce. Nevertheless, in the occupational context, this technology is mainly based on non-invasive BCIs, specifically EEG technology. Therefore, BCIs seem to have great potential for future industry safety applications, especially in processes where cognitive variables of workers, such as attention, are relevant.

The conclusions regarding the specific objective to explore the BCIs as an emerging risk are as follows:

- ***A general pre-assessment of the BCI technology has been defined.*** Such is configured by the qualitative results of the type of emerging risk, level of emerging risk, and the strategies for emerging risk management.
- ***The type of BCI as an emerging risk is a new risk.*** Such typification is for two reasons. Firstly, this device can consider a risk that did not previously exist and is caused by one new technology. Secondly, although the risk seems to be increasing, it is too early to state that the risk increases according to the growth phase.
- ***The level of emerging risk is high***. This level is high due to the combination of a high degree of uncertainty (Q) and high potential consequences (C). The high degree of uncertainty (Q) is the result of low quality of knowledge (K) and low level of understanding (N).
- ***The strategies for this emerging risk management are broad and complex.***

These conclusions define an emerging field of study for safety and security fields. However, these conclusions are mainly limited by three interrelated methodological factors: the bibliographic review method and the generic and qualitative characteristics that have been considered of the BCIs technology.

Three future lines are proposed to overcome these limitations. In the first place, with the basis defined in this work, can be designed other scoping studies complementary or systematic bibliographic reviews. Various taxonomies and standardization work based on specific terms, concepts, and technologies can be pursued with such reviews. Second, the approach shown in Fig. 7 is capable of being modeled generically or specifically to design techniques to assess statically or dynamically the BCI risks. In such modeling, the uncertainty variable could be integrated as a third axis to analyze risk as an emerging risk. Such a modeling approach represents a multidisciplinary challenge for safety and security fields. Third, based on the previous suggestions, as well as the foundations proposed on the concepts "BCIs risks," "BCI security," and "BCI safety," future research works can be developed with which to identify specific BCIs risks considering the relationship between the technology of humans and industrial safety.

Finally, the greatest challenge lies in defining the tolerability criteria of individual and social risk. In addition, it is essential to differentiate between specific technologies, their costs, and their benefits.

CRediT authorship contribution statement

F. Brocal: Writing – review & editing, Writing – original draft, Resources, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

None

Appendix

(See Table A1).

Table A1
Bibliometric characteristics.

N°	Authors	Title	Document Type	Safety			Security	
				Risk identification	Fatigue detection	Safety control	Cyber-attacks	Authen-tication
1	(Alomari et al., 2017)	What your brain says about your password: Using brain-computer interfaces to predict password memorability	Proc. Paper					●
2	(Bahr et al., 2011)	Cyber Risks to Secure and Private Universal Access	Proc. Paper				●	
3	(Belkacem & IEEE, 2020)	Cybersecurity Framework for P300-based Brain Computer Interface	Proc. Paper				●	
4	(Bellman et al., 2018)	On the potential of data extraction by detecting unaware facial recognition with brain-computer interfaces	Conf. paper				●	
5	(Bernal et al., 2020)	Cyberattacks on Miniature Brain Implants to Disrupt Spontaneous Neural Signaling	Article				●	
6	(Bernal et al., 2021)	Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges	Article				●	
7	(Bernal et al., 2022)	Neuronal Jamming cyberattack over invasive BCIs affecting the resolution of tasks requiring visual capabilities	Article				●	
8	(Bhalerao et al., 2020)	Protection of BCI system via reversible watermarking of EEG signal	Article				●	
9	(Bonaci et al., 2015)	Securing the Exocortex: A Twenty-First Century Cybernetics Challenge	Article				●	
10	(Chen et al., 2016)	A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes	Article					●
11	(Dehais et al., 2018)	Assessing working memory load in real flight condition with wireless fNIRS	Book chap.		●			
12	(Gladden, 2016)	Neuromarketing applications of neuroprosthetic devices: an assessment of neural implants' capacities for gathering data and influencing behavior	Proc. Paper				●	
13	(Han et al., 2019)	Recognition of Pilot's Cognitive States based on Combination of Physiological Signals	Proc. Paper		●			
14	(Huang et al., 2021)	Virtual reality safety training using deep EEG-net and physiology data	Article	●				
15	(Karim et al., 2019)	A Trusted Bluetooth Performance Evaluation Model for Brain Computer Interfaces	Proc. Paper				●	
16	(Kaur et al., 2020)	A study of EEG for enterprise multimedia security	Article					●
17	(Kim et al., 2021)	Development of an Information Security-Enforced EEG-Based Nuclear Operators' Fitness for Duty Classification System	Article	●				
18	(Klein, 2016)	Informed Consent in Implantable BCI Research: Identifying Risks and Exploring Meaning	Article	●				
19	(Klein & Ojemann, 2016)	Informed consent in implantable BCI research: identification of research risks and recommendations for development of best practices	Article	●				
20	(Landau et al., 2020)	Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space	Article				●	
21	(Lange et al., 2018)	Side-channel attacks against the human brain: the PIN code case study (extended version)	Article				●	
22	(Lee & Yoo, 2012)	A Development of Cognitive Assessment Tool based on Brain-Computer Interface for Accident Prevention	Article	●				
23	(Li et al., 2015)	Brain-Computer Interface Applications: Security and Privacy Challenges	Proc. Paper				●	
24	(Li et al., 2020)	Sliding-Mode Nonlinear Predictive Control of Brain-Controlled Mobile Robots	Article			●		
25	(Liu et al., 2015)	Assessment of Mental Fatigue: An EEG-based Forecasting System for Driving Safety	Proc. Paper		●			
26	(Liu et al., 2016)	Driving Fatigue Prediction with Pre-Event Electroencephalography (EEG) via a Recurrent Fuzzy Neural Network	Proc. Paper		●			
27	(Merrill et al., 2019)	One-Step, Three-Factor Passthought Authentication With Custom-Fit, In-Ear EEG	Article					●

(*continued on next page*)

Table A1 (*continued*)

N°	Authors	Title	Document Type	Safety			Security	
				Risk identification	Fatigue detection	Safety control	Cyber-attacks	Authen-tication
28	(Min & Cai, 2020)	Driver Fatigue Detection Based on Multi-scale Wavelet Log Energy Entropy of Frontal EEG	Article		●			
29	(Ming et al., 2021)	EEG-Based Drowsiness Estimation for Driving Safety Using Deep Q-Learning	Article		●			
30	(Moioli et al., 2021)	Neurosciences and Wireless Networks: The Potential of Brain-Type Communications and Their Applications	Article				●	
31	(Morales & Morgera, 2009)	Integrated sensing biosystems	Conf. paper				●	
32	(Moreno-Rodriguez et al., 2021)	BIOMEX-DB: A Cognitive Audiovisual Dataset for Unimodal and Multimodal Biometric Systems	Article					●
33	(Narayana et al., 2019)	Mind your thoughts: BCI using single EEG electrode	Article					●
34	(Neu et al., 2019)	Cognitive work protection—A new approach for occupational safety in human-machine interaction	Book chap.			●		
35	(Penaloza et al., 2015)	Brain signal-based safety measure activation for robotic systems	Article			●		
36	(Pittman et al., 2018)	Curating Research Data - Cyber security perspective from a nascent Brain Machine Interface Laboratory	Proc. Paper				●	
37	(Sciaraffa et al., 2020)	The evolution of passive brain-computer interfaces: Enhancing the human-machine interaction	Book chap.	●				
38	(She et al., 2020)	Multi-class motor imagery EEG classification using collaborative representation-based semi-supervised extreme learning machine	Article			●		
39	(Sourin et al., 2016)	Problems of Human-Computer Interaction in Cyberworlds	Proc. Paper					●
40	(Tsai, 2017a)	Applying Physiological Status Monitoring in Improving Construction Safety Management	Article		●			
41	(Tsai, 2017b)	Enhancing nuclear power plant safety via on-site mental fatigue management antenna	Article		●			
42	(Wester et al., 2013)	Experimental Validation of Imposed Safety Regions for Neural Controlled Human Patient Self-Feeding using the Modular Prosthetic Limb	Proc. Paper			●		
43	(Witkowski et al., 2014)	Enhancing brain-machine interface (BMI) control of a hand exoskeleton using electrooculography (EOG)	Article			●		
44	(Xia & Fan, 2020)	Security Analysis of Sports Injury Medical System Based on Internet of Health Things Technology	Article				●	
45	(Yang, 2019)	A Study on Development of EEG-Based Password System Fit for Lifecaretainment	Article					●
46	(Zhang et al., 2016)	A Vehicle Active Safety Model: Vehicle Speed Control Based on Driver Vigilance Detection Using Wearable EEG and Sparse Representation	Article		●			
47	(Zhang et al., 2017)	Design of a Fatigue Detection System for High-Speed Trains Based on Driver Vigilance Using a Wireless Wearable EEG	Article		●			
48	(Zhou et al., 2021)	Hazard differentiation embedded in the brain: A near-infrared spectroscopy-based study	Article	●				
n				**7**	**10**	**6**	**17**	**8**

References

Alomari, R., Martin, M. V., MacDonald, S., Bellman, C., Liscano, R., Maraj, A., & IEEE. (2017). *What your brain says about your password: Using brain-computer interfaces to predict password memorability*10.1109/PST.2017.00024.

Arksey, H., O'Malley, L., 2005. Scoping studies: towards a methodological framework. Null 8 (1), 19–32. https://doi.org/10.1080/1364557032000119616.

Bahr, G. S., Mayron, L. M., & Gacey, H. J. (2011). In Stephanidis C. (Ed.), *Cyber Risks to Secure and Private Universal Access*.

Belkacem, A. N., & IEEE. (2020). *Cybersecurity Framework for P300-based Brain Computer Interface*.

Bellman, C., Martin, M. V., MacDonald, S., & IEEE. (2018). *On the Potential of Data Extraction by Detecting Unaware Facial Recognition with Brain-Computer Interfaces*10.1109/ICCC.2018.00022.

Bernal, S.L., Celdran, A.H., Maimo, L.F., Barros, M.T., Balasubramaniam, S., Perez, G.M., 2020. Cyberattacks on Miniature Brain Implants to Disrupt Spontaneous Neural Signaling. Ieee Access 8, 152204–152222. https://doi.org/10.1109/ACCESS.2020.3017394.

Bernal, S.L., Celdran, A.H., Perez, G.M., Barros, M.T., Balasubramaniam, S., 2021. Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. *Acm.* Computing Surveys 54(1)10.1145/3427376.

Bernal, S.L., Celdrán, A.H., Pérez, G.M., 2022. Neuronal Jamming cyberattack over invasive BCIs affecting the resolution of tasks requiring visual capabilities. Computers & Security 112, 102534. https://doi.org/10.1016/j.cose.2021.102534.

Bhalerao, S., Ansari, I.A., Kumar, A., 2020. Protection of BCI system via reversible watermarking of EEG signal. Electronics Letters 56 (25), 1389–U30. https://doi.org/10.1049/el.2020.2532.

Peter Blokland, & Genserik Reniers. (2017). Safety and Performance Total Respect Management (TR^3M): A Novel Approach to Achieve Safety and Performance Proactively in Any Organisation. Nova Science Publishers.

Bonaci, T., Herron, J., Matlack, C., Chizeck, H.J., 2015. Securing the Exocortex: A Twenty-First Century Cybernetics Challenge. IEEE Technology and Society Magazine 34 (3), 44–51. https://doi.org/10.1109/MTS.2015.2461152.

Bonci, A., Fiori, S., Higashi, H., Tanaka, T., Verdini, F., 2021. An Introductory Tutorial on Brain-Computer Interfaces and Their. Applications. 10 (5).

Brocal, F., Sebastián, M.A., González, C., 2017. Theoretical framework for the new and emerging occupational risk modeling and its monitoring through technology lifecycle of industrial processes. Safety Science 99, 178–186. https://doi.org/10.1016/j.ssci.2016.10.016.

Brocal, F., González, C., Sebastián Pérez, M.Á., 2018. Technique to identify and characterize new and emerging risks: A new tool for application in manufacturing processes. Elsevier. https://doi.org/10.1016/j.ssci.2018.05.005.

Brocal, F., Paltrinieri, N., González-Gaya, C., Sebastián, M.A., Reniers, G., 2021. Approach to the selection of strategies for emerging risk management considering uncertainty as the main decision variable in occupational contexts. Safety Science 134, 105041. https://doi.org/10.1016/j.ssci.2020.105041.

Burwell, S., Sample, M., & Racine, E. (2017). Ethical aspects of brain computer interfaces: a scoping review.*18*.

Chen, Y.Y., Atnafu, A.D., Schlattner, I., Weldtsadik, W.T., Roh, M.C., Kim, H.J., Lee, S.W., Blankertz, B., Fazli, S., 2016. A High-Security EEG-Based Login System with RSVP

Stimuli and Dry Electrodes. Ieee Transactions on Information Forensics and Security 11 (12), 2635–2647. https://doi.org/10.1109/TIFS.2016.2577551.
Coates McCall, I., Lau, C., Minielly, N., Illes, J., 2019. Owning Ethical Innovation: Claims about Commercial Wearable Brain Technologies. Neuron 102 (4), 728–731. https://doi.org/10.1016/j.neuron.2019.03.026.
Dehais, F., Ayaz, H., & Gateau, T. (2018). Assessing working memory load in real flight condition with wireless fNIRS. *Neuroergonomics: The Brain at Work and in Everyday Life* (pp. 213-214)10.1016/B978-0-12-811926-6.00041-5.
Denning, T., Matsuoka, Y., Kohno, T., 2009. Neurosecurity: security and privacy for neural devices. Neurosurgical Focus 27(1)10.3171/2009.4.FOCUS0985.
Gladden, M. E. (2016). In Vrontis D., Weber Y. and Tsoukatos E.(Eds.), *Neuromarketing applications of neuroprosthetic devices: an assessment of neural implants' capacities for gathering data and influencing behavior*.
Han, S. Y., Kim, J. W., Lee, S. W., & IEEE. (2019). *Recognition of Pilot's Cognitive States based on Combination of Physiological Signals*.
L. R. Hochberg, & J. P. Donoghue. (2006). *Sensors for brain-computer interfaces*10.1109/MEMB.2006.1705745.
Huang, D.J., Wang, X.L., Liu, J.H., Li, J.Y., Tang, W., 2021. Virtual reality safety training using deep EEG-net and physiology data. Visual Computer. https://doi.org/10.1007/s00371-021-02140-3.
International Organization for Standardization (ISO), 2017. Ergonomic principles related to mental workload — Part 1: General issues and concepts, terms, and definitions. ISO 10075-1. ISO, Geneva.
Karim, H., Rawat, D. B., & IEEE, C. S. (2019). *A Trusted Bluetooth Performance Evaluation Model for Brain Computer Interfaces*10.1109/IRI.2019.00021.
Kaur, B., Singh, D., Roy, P.P., 2020. A study of EEG for enterprise multimedia security. Multimedia Tools and Applications 79 (15–16), 10805–10823. https://doi.org/10.1007/s11042-020-08667-2.
Kim, J.H., Cho, Y., Suh, Y.A., Yim, M.S., 2021. Development of an Information Security-Enforced EEG-Based Nuclear Operators' Fitness for Duty Classification System. Ieee Access 9, 72535–72546. https://doi.org/10.1109/ACCESS.2021.3078470.
Klein, E., 2016. Informed Consent in Implantable BCI Research: Identifying Risks and Exploring Meaning. Science and Engineering Ethics 22 (5), 1299–1317. https://doi.org/10.1007/s11948-015-9712-7.
Klein, E., Ojemann, J., 2016. Informed consent in implantable BCI research: identification of research risks and recommendations for development of best practices. Journal of Neural Engineering 13(4)10.1088/1741-2560/13/4/043001.
Kristensen, V., Aven, T., Ford, D., 2006. A new perspective on Renn and Klinke's approach to risk evaluation and management. Reliability Engineering & System Safety 91 (4), 421–432. https://doi.org/10.1016/j.ress.2005.02.006.
Landau, O., Puzis, R., Nissim, N., 2020. Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space. Acm Computing Surveys 53(1) 10.1145/3372043.
Lange, J., Massart, C., Mouraux, A., Standaert, F., -., 2018. Side-channel attacks against the human brain: the PIN code case study (extended version). Brain Informatics 5(2) 10.1186/s40708-018-0090-1.
Lee, C., & Yoo, S. (2012). A Development of Cognitive Assessment Tool based on Brain-Computer Interface for Accident Prevention. *Journal of the Korea Safety Management & Science, 14*(1), 1-6.
Levac, D., Colquhoun, H., O'Brien, K.K., 2010. Scoping studies: advancing the methodology. Implementation Science 5 (1), 69. https://doi.org/10.1186/1748-5908-5-69.
Li, H., Bi, L., Yi, J., 2020. Sliding-Mode Nonlinear Predictive Control of Brain-Controlled Mobile Robots. IEEE Transactions on Cybernetics. https://doi.org/10.1109/TCYB.2020.3031667.
Li, Q.Q., Ding, D., Conti, M., 2015. & IEEE. Brain-Computer Interface Applications, Security and Privacy Challenges.
Liu, Y. T., Lin, Y. Y., Wu, S. L., Hsieh, T. Y., Lin, C. T., & IEEE. (2015). *Assessment of Mental Fatigue: An EEG-based Forecasting System for Driving Safety*10.1109/SMC.2015.561.
Liu, Y. T., Wu, S. L., Chou, K. P., Lin, Y. Y., Lu, J., Zhang, G. Q., Lin, W. C., Lin, C. T., & IEEE. (2016). *Driving Fatigue Prediction with Pre-Event Electroencephalography (EEG) via a Recurrent Fuzzy Neural Network*.
Marcus, S. (2002). Neuroethics: mapping the field: conference proceedings, May 13-14, 2002, San Francisco, California.
Merrill, N., Curran, M. T., Gandhi, S., & Chuang, J. (2019). One-Step, Three-Factor Passthought Authentication With Custom-Fit, In-Ear EEG. *Frontiers in Neuroscience, 13*10.3389/fnins.2019.00354.
Min, J., Cai, M., 2020. Driver Fatigue Detection Based on Multi-scale Wavelet Log Energy Entropy of Frontal EEG. [基于前额脑电多尺度小波对数能量熵的驾驶疲劳检测分析]. Zhongguo Gonglu Xuebao/China Journal of Highway and Transport 33 (6), 182–189. https://doi.org/10.19721/j.cnki.1001-7372.2020.06.017.
Ming, Y.R., Wu, D.R., Wang, Y.K., Shi, Y.H., Lin, C.T., 2021. EEG-Based Drowsiness Estimation for Driving Safety Using Deep Q-Learning. Ieee Transactions on Emerging Topics in Computational Intelligence 5 (4), 583–594. https://doi.org/10.1109/TETCI.2020.2997031.
Moioli, R.C., Nardelli, P., Barros, M.T., Saad, W., Hekmatmanesh, A., Silva, P., de Sena, A.S., Dzaferagic, M., Siljak, H., Van Leekwijck, W., Melgarejo, D.C., Latre, S., 2021. Neurosciences and Wireless Networks: The Potential of Brain-Type Communications and Their Applications. Ieee Communications Surveys and Tutorials 23 (3), 1599–1621. https://doi.org/10.1109/COMST.2021.3090778.
Morales, G.J., Morgera, S.D., 2009. Integrated sensing biosystems. Paper presented at the *IFMBE Proceedings* 24, 141–142.
Moreno-Rodriguez, J.C., Atenco-Vazquez, J.C., Ramirez-Cortes, J.M., Arechiga-Martinez, R., Gomez-Gil, P., Fonseca-Delgado, R., 2021. BIOMEX-DB: A Cognitive Audiovisual Dataset for Unimodal and Multimodal Biometric Systems. Ieee Access 9, 111267–111276. https://doi.org/10.1109/ACCESS.2021.3100035.
Narayana, S., Prasad, R.V., Warmerdam, K., 2019. Mind your thoughts: BCI using single EEG electrode. Iet Cyber-Physical Systems: Theory & Applications 4 (2), 164–172. https://doi.org/10.1049/iet-cps.2018.5059.
Neu, C., Kirchner, E. A., Kim, S. -., Tabie, M., Linn, C., & Werth, D. (2019). Cognitive work protection—A new approach for occupational safety in human-machine interaction. *Lecture Notes in Information Systems and Organisation, 29*, 211-220. 10.1007/978-3-030-01087-4_26.
Parasuraman, R., 2003. Neuroergonomics: Research and practice. Null 4 (1–2), 5–20. https://doi.org/10.1080/14639220210199753.
Penaloza, C.I., Mae, Y., Kojima, M., Arai, T., 2015. Brain signal-based safety measure activation for robotic systems. Advanced Robotics 29 (19), 1234–1242. https://doi.org/10.1080/01691864.2015.1057615.
Pittman, J.M., Bajwa, G., Joseph, J., Keller, N., 2018. Curating Research Data - Cyber Security Perspective From a Nascent Brain Machine Interface Laboratory.
Ramsey, N. F. (2020). Chapter 1 - Human brain function and brain-computer interfaces. *Handbook of Clinical Neurology, 168*, 1-13. https://doi.org/10.1016/B978-0-444-63934-9.00001-9.
Roelfsema, P.R., Denys, D., Klink, P.C., 2018. Mind Reading and Writing: The Future of Neurotechnology. Trends in Cognitive Sciences 22 (7), 598–610. https://doi.org/10.1016/j.tics.2018.04.001.
Sciaraffa, N., Aricò, P., Borghini, G., Di Flumeri, G., Di Florio, A., & Babiloni, F. (2020). The evolution of passive brain-computer interfaces: Enhancing the human-machine interaction. *Neurotechnology* (pp. 155-179)10.1049/pbhe019e_ch6.
She, Q.S., Zou, J., Luo, Z.Z., Nguyen, T., Li, R.H., Zhang, Y.C., 2020. Multi-class motor imagery EEG classification using collaborative representation-based semi-supervised extreme learning machine. Medical & Biological Engineering & Computing 58 (9), 2119–2130. https://doi.org/10.1007/s11517-020-02227-4.
Sourin, A., Earnshaw, R., Gavrilova, M., Sourina, O., 2016. *Problems of Human-Computer interaction in Cyberworlds*10.1007/978-3-662-53090-0_1.
Summerer, L., Izzo, D., & Rossini, L. (2009). Chapter 16 Brain–Machine Interfaces for Space Applications—Research, Technological Development, and Opportunities. *International Review of Neurobiology, 86*, 213-223. https://doi.org/10.1016/S0074-7742(09)86016-9.
Tsai, M.K., 2017a. Applying Physiological Status Monitoring in Improving Construction Safety Management. Ksce Journal of Civil Engineering 21 (6), 2061–2066. https://doi.org/10.1007/s12205-016-0980-9.
Tsai, M.K., 2017b. Enhancing nuclear power plant safety via on-site mental fatigue management. Nuclear Technology & Radiation Protection 32 (1), 109–114. https://doi.org/10.2298/NTRP1701109T.
Vosviewer, 2022. Vosviewer for Windows, Version 1.6.18. The Netherlands. URL: https://www.vosviewer.com/.
Wester, B.A., Para, M.P., Sivakumar, A., Kutzer, M.D., Katyal, K.D., Ravitz, A.D., Beaty, J. D., McLoughlin, M.P., Johannes, M.S., 2013. Experimental Validation of Imposed Safety Regions for Neural Controlled Human Patient Self-Feeding using the Modular Prosthetic Limb.
Wexler, A. (2020). Chapter Five - Do-it-yourself and direct-to-consumer neurostimulation. *Developments in Neuroethics and Bioethics, 3*, 127-155. https://doi-org.ezproxy.uned.es/10.1016/bs.dnb.2020.03.005.
Witkowski, M., Cortese, M., Cempini, M., Mellinger, J., Vitiello, N., Soekadar, S.R., 2014. Enhancing brain-machine interface (BMI) control of a hand exoskeleton using electrooculography (EOG). Journal of Neuroengineering and Rehabilitation.
Wolpaw, J. R., Millán, J. d. R., & Ramsey, N. F. (2020). Chapter 2 - Brain-computer interfaces: Definitions and principles. *Handbook of Clinical Neurology, 168*, 15-23. https://doi-org.ezproxy.uned.es/10.1016/B978-0-444-63934-9.00002-0.
World Health Organization. (2020). *Basic documents: forty-ninth edition (including amendments adopted up to 31 May 2019)* (Forty-ninth ed.). Geneva: World Health Organization.
Xia, Y.P., Fan, Y.X., 2020. Security Analysis of Sports Injury Medical System Based on Internet of Health Things Technology. Ieee Access 8, 211358–211370. https://doi.org/10.1109/ACCESS.2020.3039262.
Yang, G., 2019. A Study on Development of EEG-Based Password System Fit for Lifecaretainment. Journal of Korea Entertainment Industry Association 13 (8), 525–530.
Zhang, X.L., Li, J.L., Liu, Y.G., Zhang, Z.T., Wang, Z.J., Luo, D.Y., Zhou, X., Zhu, M.K., Salman, W., Hu, G.D., Wang, C.B., 2017. Design of a Fatigue Detection System for High-Speed Trains Based on Driver Vigilance Using a Wireless Wearable EEG. Sensors 17(3)10.3390/s17030486.
Zhang, Z.T., Luo, D.Y., Rasim, Y., Li, Y.J., Meng, G.J., Xu, J., Wang, C.B., 2016. A Vehicle Active Safety Model: Vehicle Speed Control Based on Driver Vigilance Detection Using Wearable EEG and Sparse Representation. Sensors 16(2)10.3390/s16020242.
Zhou, X. S., Hu, Y. N., Liao, P. C., & Zhang, D. (2021). Hazard differentiation embedded in the brain: A near-infrared spectroscopy-based study. *Automation in Construction, 122*10.1016/j.autcon.2020.103473.