# The impact of the human dimension on decision support systems

**Aurelian BUZDUGAN, Gheorghe CAPATANA**

Moldova State University

aurelian.buzdugan@yahoo.com; gh_capatana@yahoo.com

**Abstract:** The human dimension has a critical role in the development and use of decision support systems. In order to ensure that the quality and performance of computer-supported decisions is high, the human dimension needs to be assessed during all phases of system development. Furthermore, the domain and context in which the systems will be used may impose additional requirements. For example, domains in which safety and security are a primary concern require continuous training of users and advanced systems that are adjusted to the requirements. In this paper, we will evaluate the implication of the human dimension within a decision support system for cyber risk management in critical infrastructures. We will analyze the impact that this dimension has upon the decision support systems and propose solutions on how to overcome or better manage known limitations caused by the elements of the human factor. We will discuss also how the proposed solutions and recommendations can increase the efficiency of decision support systems used in critical infrastructures.

**Keywords:** human dimension, information systems, decision support systems, cyber security.

# Impactul dimensiunii umane asupra sistemelor suport decizionale

**Rezumat:** Dimensiunea umană are un rol critic în dezvoltarea și utilizarea sistemelor suport decizionale. Pentru a asigura calitatea și performanța deciziilor recomandate de un astfel de sistem, dimensiunea umană trebuie evaluată în toate fazele dezvoltării sistemului. În plus, domeniul și contextul în care vor fi utilizate aceste sisteme pot impune cerințe suplimentare. De exemplu, domeniile în care siguranța și securitatea sunt o preocupare principală, implică formarea continuă a utilizatorilor și adaptarea sistemelor conform cerințelor. În această lucrare, vom evalua implicațiile dimensiunii umane în cadrul unui sistem de suport a deciziilor pentru gestionarea riscurilor cibernetice în infrastructurile critice. Vom analiza impactul pe care factorul uman îl are asupra sistemelor suport decizionale și vom propune soluții pentru depășirea limitărilor cauzate de elementele factorului uman. Vom discuta, de asemenea, modul în care soluțiile și recomandările propuse pot spori eficiența sistemelor de suport decizionale utilizate în cadrul infrastructurilor critice.

**Cuvinte cheie:** dimensiunea umană, sisteme informaționale, sistem suport decizional, securitate cibernetică.

## 1. Introduction

Our whole life is based on decisions, we decide on what food to eat, which route to take to get to work or what to dress depending on weather forecast or daily agenda. Besides the context and factors that influence our decision-making result, we, as the human factor, have a key role in interpreting and perceiving the context, identifying the desired decision and ultimately taking the decision. Any of the actions listed above could have similar or different results for any of us, in the same context.

There is no universal definition for describing the human dimension. Within the scope of this paper, we define and interpret the human dimension as the multitude of aspects that describe human activities, from ethics to knowledge. We find that the term “human factor elements” is similar to the “human dimension” one, and it refers to notions as comprehension, interpretation, perception, abilities to perform a task or even to describe the physical state.

The evaluation and integration of the human dimension during the development of a decision support system (DSS) becomes a challenging task, as a broad spectrum of variables related to this factor have to be taken into account. In the context of systems used in safety or security related environments (Buzdugan A. A & Buzdugan A. I., 2016), such as critical infrastructures (CI), the human factor elements have an even higher priority and importance. CI domains exemplified in

https://doi.org/10.33436/v31i3y202103

Figure 1, are considered vital for citizens' health, safety and financial wellbeing. These areas of activities are fundamental for the functioning and development of economy, public administration and even national security. Therefore, any unauthorized intervention, disruption or destruction of the information technology (IT) equipment within a CI could lead to operational risks with a security or even safety impact. This also applies to CIs to which a country is dependant upon, and not necessary directly owned or controlled (Bucovetschi et al., 2018).

The role of the human dimension proliferates sharply in all aspects of the CI domain. In this paper, we explore the peculiarities of the human factor elements and their impact upon the efficiency of an information system, as we have identified that this element is not adequately addressed at the design phase (Buzdugan, 2020). We will also evaluate these aspects in relation to a proposed DSS as a viable solution to support the decision-making process in managing cyber risks in the CI domain. The human dimension can therefore impact the security of a system, both positively and negatively (Nixon, 2013). The interface, as an example, can support the users in taking better decisions. Moreover, the specific context of the DSS dictates the assessment of human behavior when it comes to protecting vulnerable systems (Khripunov, 2014). Taking this into account, we will evaluate both the positive and negative impact of the human dimension upon information systems.

The remaining of this paper is structured as follows: the second chapter represents a review on the human element factors in relation to the DSS. In chapter three we will describe the impact of these elements in security and safety domains, while in chapter four we will discuss the possibility of automating decision-making process as a solution to overcoming known human factor errors. We will conclude with the main takeaways from the performed analysis, and with recommendations on how to more effectively consider the human dimension starting with the design phase, as well as propose future research directions.

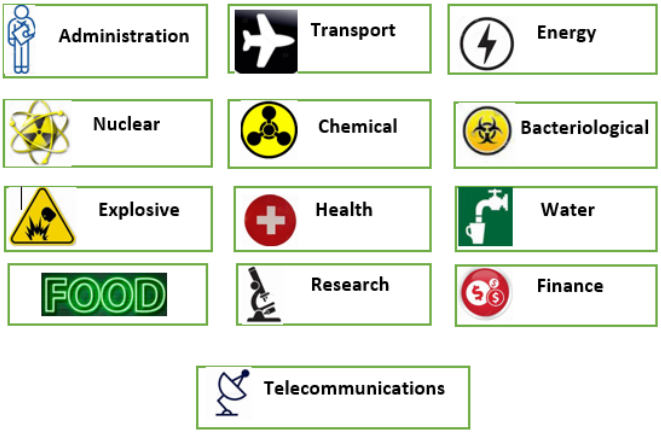


**Figure 1.** Critical Infrastructure domains

## 2. Human dimension and DSS

In this chapter we will discuss the common impact that the human dimension has upon information systems, as well as typical solutions to overcome the negative effects.

The human dimension has a critical role in the development and use of decision support systems (Buzdugan & Capatana 2020; Buzdugan, 2020). The element of professional culture, which involves knowledge about the specific domain, abilities required to use the DSS efficiently as well as the format and content that is displayed by the presentation system, play continuous and major roles in achieving the scope and efficiency of the proposed DSS. In order to manage cyber risks, specialized and up-to-date knowledge of risks and mitigations is needed to control these risks more efficiently. Integrating this process in CI domain, sets specific requirements for the results delivered by the DSS. Below we will explore the impact of the human factor elements upon the DSS language and the presentation system.

The in scope DSS for cyber risk management in CI domain can be characterized as a smart, collaborative, user-centric information system that adapts to the user profile. One solution to overcome known human factor limitations is to adjust the results based on the user role. This represents one of the proposed capabilities of the user interface, which can be seen as an extension of adaptability. The user profile data is an invaluable data source that can be extremely useful in overcoming known constraints created by the human dimension. This data, and the knowledge built around it, could be stored as part of the user profile data type, suggested by us to be part of the language system (Buzdugan, 2020). Having results adapted to a specific role directly relates to the format and content of the data presented by the DSS. Below are some examples.

**Developers** need to see technical data and how the system operates in real time, in order to check and adjust the code as part of his/her duties;

**Decision-makers** require strategic information regarding identified cyber risks, potential impact, reputation, estimated costs to mitigate and other type of high-level data. Based on the scope of the proposed DSS, this role is overseeing the risk management process, it is informed about the outcome and progress of the mitigation, or can request any other inputs from other roles, such as from the operators;

**Operators** would need technical data regarding the cyber risks, affected digital assets, dependencies with other assets and guidance to mitigate or contain this risk and also the ability to collaborate with others. We note, that this would be the profile that requires complex technical results that can inter alia include - the projected state of the system, implementation progress for mitigations, guidelines or procedures from the vendors, as well as the ability to cooperate with any other roles during these processes. A clear and intuitive system would tremendously support the tasks performed by the operator role, and minimize any potential safety incidents.

Any major deviations in the presentation system in terms of format, content and relevance to the roles could be a risk towards the acceptance of the DSS. This can have significant implications on the operations, security and safety of the CI. Filip defined this risk as system opacity in which the output is not adapted to the role: either there is too much or not enough information, either sufficient but presented in a confusing manner (Filip, 2012).

Another solution that would improve the perceived efficiency of the DSS is the simplicity of the user interface. We believe that by showing clear answers and providing an intuitive interface, information systems benefit from a greater success and adoption rate. The easier it is to find and read the information regarding a cyber risk, such as description, dependencies, impact, cost and mitigations - the more likely this risk will be understood properly by the user, and eventually controlled efficiently. This characteristic of the user interface can have a direct impact on the actual, perceived, efficiency of the DSS.

We have also argued about the necessity to build the DSS as a module for interoperability and to facilitate adoption by other risk management methodologies (Buzdugan & Capatana, 2020). We believe common standards and taxonomies for data exchange can be used to achieve this, as well as reduce costs and provide interoperability functionalities. Similarly, standards can be used in the process of design and development of the user interfaces, whilst following best practices and recommendations in terms of user-friendly design.

As per Filip, the ISO 9241 standard can be seen as an useful, usable and used solution for the DSS interfaces (Filip et al., 2017). This standard series relates to hardware and software-ergonomics aspects for the human interaction with the system (ISO 9241, 2010). The different modules of the standard relate to requirements on how to use the keyboard, menus, command dialogues, as well as go deeper into more specialized areas such as human-centered design, accessibility, electronic visual displays, tactile or haptic interaction and even design aspects for physical input devices (ISO 9241, 2010). Using such standards is a forward-looking solution. This ensures that a modern DSS benefits from the same friendly and usable interface even if using emerging technologies. Some of these technologies or concepts can be biometrics (voice/ speech/ face recognition), virtual reality or augmented reality. In case of specific requirements, any user interface can be further adjusted or enhanced based on needs or regulations of each enterprise.

Perception is another element relating to the human factor. In our context, this refers to the assessment of the results provided by the DSS as well as the understanding of the actual data. Perception process is directly linked to the quality of comprehension, estimation and assessment of the actual cyber risk or mitigations. Some studies show that users are more aware of vulnerabilities for which attacks are reported more frequently (Ellerby et al., 2019), potentially due to familiarity and specific knowledge of this system based on the incident reports. On the other side, studies show that the perception of required skills and resources to conduct a cyber-attack is directly related to the estimation of a high technological maturity of a system, or no knowledge about the maturity level (Ellerby et al., 2019). Perception is one factor that can have a negative impact upon the efficiency of the information system, based on the background, culture or knowledge of the end-user.

This proves once more that the human dimension is complex, and various type of requirements have to be considered when developing the DSS or its interfaces. The requirements can also be used during regular evaluation of the system efficiency. Perception from our point of view is one of the most critical elements of the human factor, with direct repercussions on the effectiveness and quality of the risk identification and assessment process.

A framework that can support the estimation of perception is the *Technology Acceptance Model* (TAM), which can forecast the adoption of a certain technology (Davis, 1989). This model was initially used in the industrial context and later gained popularity in the assessment of information systems acceptance (Schepers & Wetzels, 2007). TAM has been used in evaluating the behavior change and adoption for new technologies such as personal computers (Venkatesh & Brown, 2001), sensory enabling technologies (Kim & Forsythe, 2008) or e-services (Lin et al. 2007). The TAM consists of two variables:

- Perceived Usefulness (PU) of the technology by the user;
- Perceived Ease of Use (PEU), which reflects the user's evaluation of how easy it is to use the technology for a specific task.

One example of the TAM application refers to passwords: a strong password has a high PU, however low PEU because passwords could be forgotten (Bossomaier, 2019). If we were to add two-factor authentication, then PEU would increase, whilst PU could increase or decrease, based on user's perception. Therefore, we note that the evaluation and corrective measures requires other factors to be considered. TAM is not necessarily a universal solution and it is recommended to be integrated as part of other models (Legris, 2003). We believe this model can also be used to describe partially the human perception in the context of information systems, especially as we propose a DSS to be used in CI domain, which is often associated to industry. This factor can be included in efficiency assessment processes. We also find that context is trivial in order to better estimate the PU and PEU. In our case this would refer to the security culture (organizational or individual), user awareness in terms of threats and impacts posed by cyber risks, user training in being able to deter or mitigate these threats, as well as the system itself (e.g., user interface, security controls, performance). In addition, the knowledge possessed by end-users in IT can facilitate to improve the user experience, as well as support a faster process of learning and adaptation to more complex interfaces (Amantini, 2012). We would add that, cross discipline cooperation between experts in IT and OT, could improve the perception overall, by developing informative interfaces suited for operational environments, as well as implementing usable processes within the information system.

Impact, self-efficacy and cost are other concepts that refer to the human dimension. The motivation to prevent or deter cyber-threats is related to the perceived threat, knowledge about the potential impact, capability to prevent it as well as the necessary cost (Huigang, 2010). If we look at the DSS as a socio-technical system, external factors towards the users, can influence the assessment of the perception, impact, and cost of even ability to deter the threat. Examples of such cases can be factors that have influence upon the psychological or physical abilities. We recommend having regular and comprehensive training conducted for DSS users, to cover all type of scenarios. Since CI domain has high operational requirements, we believe such training would

not be a burden and could be included in the regular training programs and assessments that already exist in the CI domain due to operational requirements. Moreover, we see the opportunity to use the propose DSS to aid this process. For example, this can be used in demo mode in order to support drills or training programs. This can enhance professional culture and support the internal capacity building, as well maintain the IT skills necessary to efficiently use this system.

Therefore, the DSS can support activities such as simulation or training via gamification of various cyber risk management scenarios. This can also be useful during proof-of-concept presentations in order to persuade senior management about necessary cyber security investments (adapted from Fielder et al., 2016).

We consider that the human dimension needs to be evaluated holistically. It is important to acknowledge that the human factor elements can influence upon the efficiency of the system in a positive or negative direction, depending on various factors.

## 3. Mission critical DSS

In the previous chapter we evaluated general aspects of the human dimension in relation to information systems. Most of these systems have appropriate security controls to the commodity type of cyber threats. However, the CIs represent a target to terrorist or state sponsored groups, as cyber warfare became quite common lately. Therefore, a small percentage of the information systems that consider advanced threats and that are protected against them, are necessary to be developed. In such cases, security and safety requirements prevail over costs and reputational issues. When it comes to specialized mission critical systems, the implication of the human dimension is much more complex and crucial. In this chapter, we will analyze the impact of the human factor in the context of a security and safety focused DSS. CI represents a domain where decisions could have an impact upon the society, people or even nation states. We consider cyber risk management in CI as a critical process, as decisions could impact upon the OT used in such organizations.

As the DSS is an anthropocentric system, the impact of the human dimension should be evaluated at the concept and design phases, but also throughout the regular evaluations. This can have a positive impact upon the system as it is being designed in a more secure way (adapted from Nixon, 2013). It is necessary to ensure that implemented security concepts, as well as controls, are appropriate and fit for the purpose of the system and understood by most of the users. There has to be a balance between security and usability, in order to have the best efficiency. Less usable systems, or systems where users are not able to cope with the security controls, will create less efficiency for the organization. On the other hand, a fully secure, comprehensive and accurate DSS used for cyber risk management in CIs does not guarantee the best decisions will be taken. It is up to the user of the system, such as operators or decision makers, to do the final assessment of the proposed results and make the decision. A possibility to overcome this can be through automating decision-making, that would not only support, identify or propose a decision, but will also take the best decision (Filip et al., 2017; Parasuraman et al. 2000).

In general, factors related to human behaviour can either improve or decrease the quality of decisions. Systems that are perceived as highly advanced could lead to the fact that the user is trusting more than necessary the results presented by the system. This could reduce the analytical and professional skills of the user over time (Filip et al., 2017). On the other hand, less efficient systems could tire users as a lot of information is missing or still needs to be processed. Therefore, a well-adjusted approach is mandatory when it comes to decisions that can affect safety or security.

A model that can be used to evaluate the impact of the human dimension and adjust according to the information systems for such environments is the Human Factors Integration (HFI) framework (Nixon, 2013). HFI is a framework used in the United Kingdom in order to integrate the human factor in the defense systems. HFI looks at the identification, tracking and resolving the human related issues in the development of the capability. It is necessary to mention that HFI criteria are both goal-based and risk-based. A similar concept is present in the Human

Systems Integration framework (HSI) from the United States (Pew & Mavor, 2007; Booher, 2003). Unlike HFI, HSI is based on nine domains, six of which coincide with those of HFI (Figure 2). The seventh domain of HFI (social and organizational) is in our opinion seen more complex in HSI (as survivability, habitability and environment).

We note that both frameworks focus on eliminating risks related to the human dimension, and could be used to evaluate the vectors impacting cybersecurity of highly critical systems. Certain analysis was performed on how information systems can be developed and used in defense organizations, based on HFI criteria (Nixon, 2013). We will build on the existing results and propose recommendations for the DSS in scope.

The HFI has seven domains, however the analysis was performed only on six of them that are applicable to cybersecurity. Although, we consider that the seventh domain, which is health hazards, can represent an external threat towards the end user, and therefore have an indirect impact to cybersecurity. Due to the complexity of the human dimension, we believe these domains should be considered holistically due to the interdependence. Below we will list each category and its respective findings, as well as evaluate them in relation to the DSS in scope.

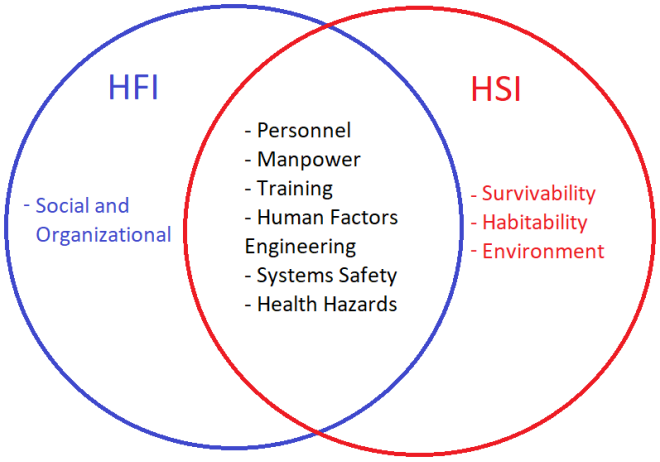


**Figure 2.** Venn diagram for HFI and HSI elements

## 3.1. Social and organizational factors

Information systems are socio-technical systems which lead to the fact that users can represent a vulnerability towards the system (Nixon, 2013). This risk is often influenced by management policies, cybersecurity culture or even the efficiency of the information systems. User motivation, work-life balance, adequate training as well as organizational leadership, are examples that positively influence employees and create a harmonic organizational culture. The lack of inclusion of these factors in cyber security risk assessments (Boyce et al., 2011) could lead to the fact that internal threats are greater than external ones (Wilding, 2007). This problem becomes even more complex when we analyze the skills, awareness, training and culture of end-users. Social and organizational factors are complex and require a holistic approach to reduce the associated risks. Combining the HFI elements with the process, people and technology (PPT) concept, it can be correlated with the role and impact of the human dimension on the organization (Figure 3). It is important to note that while it is not possible to completely eliminate risks associated with the human dimension on the organization, these can be reduced up to an acceptable level through comprehensive training and capacity building.

## 3.2. Human factors engineering and system safety

In the context of the DSS, these elements offer a perspective on how the human dimension is evaluated and integrated in the design, development, use and evaluation of the systems used in operational environments. This analysis helps optimize the interface between users and machines,

as well as ensure the safety of the system while in operation. The most efficient method to reduce threats posed by this element to include these concerns starting with the design phase.

As the quantification and measurement of the threats posed by the human dimension is hard, emerging technologies, such as biometrics, can be used to evaluate the state of the user while performing critical tasks (Nixon, 2013). Stress and pressure could lead to users taking suboptimal decisions (Dror et al., 1999; Betsch. Et al., 2003; Hahn et al., 1992; Hu et al., 2015; Hanna et al., 2016), as perception is the leading factor when it comes to identifying and preventing safety events or risks. We believe biometrics are applicable for the DSS in scope, as this technology became affordable and rather widespread (e.g., face, iris or gesture scanning).

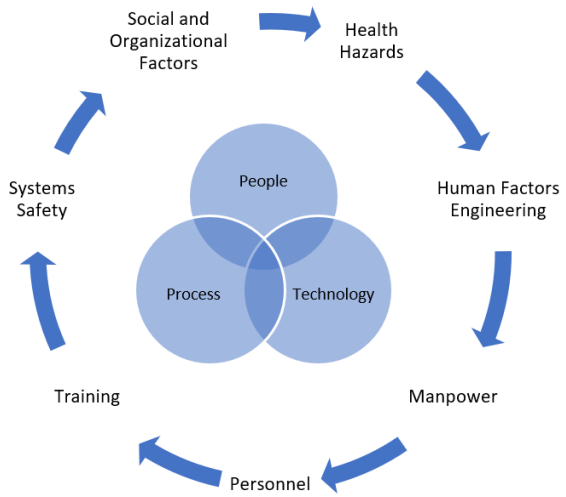


**Figure 3.** Relationship between HFI and PPT (Adapted from Anthony & Boardman, 2016)

This can be used by the DSS to identify traits that relate to a higher stress or anxiety of a user, and could be a cause for risky behaviors. Another element that could reduce risks posed by the human factor is resilience of the DSS. We believe this could be an additional solution at the application level in reducing any type of sabotage or error, being this intentional or not.

## 3.3. Manpower and personnel

Manpower defines the level of human resources available to perform a specific task (Nixon, 2013). Frequently, the scarce human and financial resources lead organizations in outsourcing critical functions as well, including cybersecurity. This can be the cause for new risks, such as increasing workload for users and decreasing the attention and investment for a specific critical task. DSS automation for certain simple and low risk tasks could help reduce this risk. However, this can have other implications, which we will discuss in the next chapter.

On the other side, information systems can produce the sense of anonymity, or that results are not happening in real life, which can trigger behavior that is not expressed in real life. This can create major safety concerns from the personnel standpoint. Organizations need to adjust existing training to cover the IT domain and inherent risks. Moreover, the possibility of a cyber attack to lead to safety incidents is still underestimated and awareness can be raised via relevant on-the-job exercises.

## 3.4. Training

Continuing education programs is the most efficient method to reduce risks posed by the human factor towards the organization. This has to be comprehensive in terms of materials and covered use cases, as well as for best results, it has to be not only employer driven (Vevera & Albescu, 2018). It is recommended to include users in the overall cyber risk management process, to raise awareness and knowledge about these risks (Nixon, 2013). Training is also recognized as an efficient solution to identify and prevent insider threats (Nixon, 2013).

A supporting strategy for training and awareness is to use standards in identifying and evaluating the process in an organization, such ISO 27001 standard (ISO 27001). In addition, competency frameworks for performing certain functions, such as Mission Essential Competencies, can also diminish the probability of human error or risks created by this factor (Symons, 2006). The probability of novice, untrained users, to engage in risky behavior is higher compared to users that have adequate training and knowledge of cyber threats (Bossomaier, 2019). Based on these findings, requirements towards skills and knowledge to perform operational tasks can be established.

The cyber security culture can be efficiently built on experience and training, as well as on periodic refresher training to assimilate good practices which were developed meanwhile. The exchange of experiences as well as getting familiar with the innovative achievements in the fields are one of the most efficient methods of risk prevention or minimization of such risks. We believe the functional requirements in terms of end-user training can be implemented in the DSS. It is also important to emphasize that cyber security training is a process, due to the dynamic characteristic of the cyber space and digitalization process that affects the CI domain (Georgescu et al., 2020)

## 4. Autonomous decision making

We mentioned several times about automation applied in decision-making, referring to autonomous decision making systems, as a potential solution to reduce occurrence or impact of known human errors. As this question comes often in the context of a DSS, we will explore the current state of art in automation. The analysis of automation requirements and impact has been found in literature (Filip et al., 2017) and different classification of tasks which could be automated has been proposed (Save & Feuerberg, 2012; Sheridan & Verplanck, 1978; Parasuraman et al., 2000). Furthermore, automation is seen as a best practice and recommendation in modern IT frameworks, such as ITILv4 for IT Service Management (Miles, 2020), or DevOps for software development (Leite et al., 2019).

The requirements to enable automation and assign the decision making to a system can be categorized depending on the type of the problem to solve (Filip et al., 2017):

- completely structured problems can be solved adequately via full automation;
- semi-structured problems are best solved with human intervention or supervision, however DSS could perform certain preliminary tasks and support the users in this sense by recommending or proposing a solution;
- unstructured problems can be solved only by using human inspiration, however DSS using emerging concepts such as artificial intelligence or data mining could also support this process for multiple aspects.

This is arguable depending on the definition and characteristic of the problem. In our context, the CI domain dictates stricter requirements as an operational environment.

Another strategy recommends to automate tasks that require skill-based behavior, whereas leave tasks requiring knowledge-based behavior to be performed by users (Sheridan 1992).

We believe these definitions can support the identification of tasks that can be safely automated for the DSS in scope. Automating activities that require skill-based decision could facilitate the work of decision makers and allow to focus on more high severity risks, which require knowledge-based behavior. It is worth mentioning that a switch towards a supervisory role does not exclude the requirement to have knowledge in operations or system engineering, on the opposite, this would be a benefit in CIs, as a cross-discipline domain, in identifying areas that can be automated.

Nonetheless of the progress in automation, the human intervention cannot be total eliminated from the DSS and should remain for tasks where creativity, knowledge usage and instinct of self-preservation are requested (adapted from Filip et al., 2017). We consider this is required by the CI

domain, as cyber risks management is a process that requires creativity and thorough analysis, especially in contexts linked to CI. By comparing existing automation in other similar environments, such as NASA, we notice that the same approach is taken (Green et al., 2012). It is worth mentioning that automation does not fully exclude the human dimension. As automation is implemented and developed by users, the scenario is possible, when decisions are left at the end user's discretion when developers have no sufficient expertise in automating a specific task, is possible (Filip et al., 2017). However, from a high-level perspective, we ascertain that such risks could be reduced by ensuring that developer teams have sufficient expertise, as well as joint task-forces are created to evaluate the final created products.

Cyber risk management constitutes a complex process looking at a large number of variables. As the number of the cyber risks is continuously growing, this could be a better cooperation between decision makers and operators in identifying tasks that can be automated. In addition, the cooperation between all the stakeholders can lead to better informed decisions for areas where investment in automation would lead to efficiency gains and cost savings. Another benefit to maintain human intervention in the DSS is to preserve a quality of professional life of the end user. Such systems are required to be useful and usable, but also keep stimulating the end-users to think analytically and critically in order to improve the overall taken decisions (Filip, 1989; Filip, 1995). We consider this would ensure that quality of automation is continuously improved, otherwise there is a risk of lack of improvements. We believe that the emergence of concepts such as AI, data mining and machine learning could change the requirements for automation. However, this could create new types of risks and concerns.

## 5. Conclusions and discussions

This paper does not represent a definitive analysis of the role of the human dimension in DSS and potential solutions. Having a multidimensional overview of the human dimension impact upon information systems helps to adequately tackle known risks or problems, as well as identify solutions. The dependence and impact of these human factor elements upon information systems are very broad. From one side, these can negatively influence and reduce the efficiency of decision making supported by DSS. From another side, by considering all the known constraints or risks starting with the design phase, one can improve and maximize the perceived efficiency offered by such a system. The identified elements are applicable to a DSS that is used in CI domain. However, we believe these results can also be applied for any other type of information system and domain.

As a general solution we re-iterate the need to design any information system based on the domain where it will be used (Buzdugan, 2019). In addition, the systems should be continuously adapted to the needs of the users, their roles in the organization as well as the context. Human factor elements such as perception, skills, ability to take correct decisions when under pressure, or professional culture play a critical role in the context of the proposed DSS.

Furthermore, common constraints such as costs, delivery time as well as organizational culture can also influence the quality of the final DSS. We also recommend to use existing standards, such as ISO 9241 or ISO 27001, as these are a good solution to reduce costs and delivery times given the fact that most of the functional requirements are covered by the standard. By following good practices, it is also possible to overcome and avoid known issues or constraints posed by the human factor elements. Moreover, modern computer technologies, such as those reading biometric parameters, represent an opportunity to minimize risks posed by the human dimension, especially in the CI domain.

We consider the DSS can also support organizational activities such as regular training or tabletop exercises. These would help raise the cybersecurity culture, but also the professional skills of the end users, which ultimately would reflect positively upon the perceived efficiency and use of the DSS.

Another potential solution to reduce certain risks or human errors in the decision-making process is automation. This has many benefits in terms of cost reduction, manpower and personnel optimization, as well as efficiency gains. However, by definition a CI does not meet the requirements to use automated decision making when managing cyber risks. Nonetheless, we believe that a certain percentage of actions can be identified for full automation. Stakeholder engagement and supervision activities are key for a safe and secure automation, but also for reducing known human errors or limitations.

The findings in this paper can be useful for anyone designing or evaluating DSS used in critical environments. The described human factor elements, as well as the proposed solutions, could be used to describe the end user culture, knowledge in order to model the perceived use and efficiency of the proposed DSS

## Acknowledgements

We thank Acad. F.G.Filip for the valuable advice, guidance and attention given within the doctoral program. The presentation of this article was possible due to the doctoral project "Decision support system for identifying and reducing cyber risks in critical infrastructures".

# REFERENCES

1. Amantini, A., Choraś, M., D'Antonio, S., Egozcue, E., Germanus, D., & Hutter, R. (2012) *The human role in tools for improving robustness and resilience of critical infrastructures.* Cognition, Technology and Work, 14(2), 143-155, DOI:10.1007/s10111-010-0171-2.
2. Anthony, M., Boardman, M. (2016) *Human Factors Integration (HFI): The Means of Considering the Human Component of Capability within Acquisition*, Retrieved from: https://www.incose.org/docs/default-source/default-document-library/incose-hsi_mod2_oct2016.pdf?sfvrsn=b53d8ec6_0
3. Betsch T., Haberstroh S., Molter B., Glockner A. (2004). *Oops, I did it again - relapse errors in routinized decision making, Organizational Behavior and Human Decision Processes*, Vol 93-1, Pages 62-74, DOI:10.1016/j.obhdp.2003.09.002
4. Booher, H.R. (2003) *Handbook on Human System Integr*ation. NJ: John Wiley & Sons.
5. Bossomaier, T., D'Alessandro, S., & Bradbury, R. (2019) *Human dimensions of cybersecurity*. (1st ed.) Taylor & Francis.
6. Boyce, M.W., Muse-Duma, K., Hettinger, L.J., Malone, T.B., Wilson, D.P., Lockett-Reynolds, J., (2011) *Human performance in cybersecurity: A research agenda*. In Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting.
7. Bucovetschi O., Georgescu A., Lazar M., Cirnu C. (2018) Securitatea națională a României în contextul infrastructurilor critice spațiale , Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, Vol. 28, No. 4, pp. 31-40.
8. Buzdugan, A. *Adequate domain-based security* [abstract], (2019) In: Book of Abstracts - Vienna Cyber Security Week 2019 - Protecting Critical Infrastructure. Vienna, Austria, Abstract nr 117.
9. Buzdugan, A., (2020) *Architecture Considerations for a Decision Support System in Cyber Risk Management*. 9th International Workshop on Soft Computing Applications (SOFA 2020), Arad, Romania (accepted, to be published).

10. Buzdugan, A., Capatana, Gh., (2020) *Factors for a decision support system in critical infrastructure cyber risk management*, Romanian Cyber Security Journal, Vol. 2(2), Pg.67-73.

11. Buzdugan, A.A., Buzdugan, A.I. (2016) *Cyber Security in the Nuclear and Radiological Domain: Case Study of Republic of Moldova*. In: Sontea V., Tiginyanu I. (eds) 3rd International Conference on Nanotechnologies and Biomedical Engineering. IFMBE Proceedings, vol 55. Springer, Singapore. DOI:10.1007/978-981-287-736-9_127

12. Davis, F. (1989) *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3): 319-340.

13. Dror, I.E., Basola, B., Busemeyer, J.R. (1999) *Decision making under time pressure: An independent test of sequential sampling models*. Memory & Cognition 27, 713-725 DOI:10.3758/BF03211564.

14. Ellerby, Z., McCulloch J., Wilson M., Wagner C. (2019) *Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security*.

15. Fielder, A., Panaousis, E., Malacaria, P., Hankina, C., Smeraldi, F. (2016) *Decision support approaches for cyber security investment*. Decision Support Systems 86, 13-23.

16. Filip, F. G. (1989) *Creativity and decision support systems.* Studies and Research in Computers and Informatics, 1 (1): 41-49.

17. Filip, F. G. (1995) *Toward more humanized real-time decision support systems*. In: Camarinha-Matos L, Afsarmanesh H eds, Balanced Automation Systems. Architectures and Design Methods. Chapman & Hall, London: p. 230-240.

18. Filip, F. G., (2012) *A decision-making perspective for designing and building information systems*, International Journal of Computers Communications & Control, Volume 7, No. 2, p 264-272.

19. Filip, F.G., Zamfirescu, C. B., Ciurea, C. (2017) *Computer-Supported Collaborative Decision-Making Series: Automation, Collaboration,* & E-Services, Volume 4, Springer, 216 pp. DOI: 10.1007/978-3-319-47221-8.

20. Georgescu A., Vevera A.V., Cirnu C. (2020) *Cyber as a Transformative Element in the Critical Infrastructure Protection Framework*, Romanian Cyber Security Journal, Vol. 1(2), Pg.37-44

21. Green, L., Alexandrov, N., Brown, S., Cerro, J., Gumbert, C., Sorokach, M., Burg, C. (2012) *Decision Support Methods and Tools*, 11th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference, DOI:10.2514/6.2006-7028.

22. Hahn, M., Lawson, R., Lee Y. (1992) *The effects of time pressure and information load on decision quality*. Psychology & Marketing, 9(5): 365-378.

23. Hanna, O., Beck, J., Pingping Z., Sommer, M., Ferrari S., Egner T. (2016) *Satisficing in split-second decision making is characterized by strategic cue discounting*. Journal of Experimental Psychology. Learning, Memory & Cognition, 42(12): 1937-1956.

24. Hu, Y., Wang, D., Pang, K., Xu G., Guo J. (2015) *The effect of emotion and time pressure on risk decision-making*. Journal of Risk Research, 18(5): 637-650.

25. Huigang, L., Yajiong X. (2010) *Understanding security behaviors in personal computer usage: A threat avoidance perspective*. Journal of the Association for Information Systems, 11(7):394-413.

26. ISO 27001 *Information security management*.

27. ISO/TR 9241-100:2010(en) *Ergonomics of human-system interaction*.

28. Khripunov, I., ed. (2014) *The Human Dimension of Security for Radioactive Sources: From Awareness to Culture*. Center for International Trade and Security, University of Georgia, Indonesia's National Nuclear Energy Agency.

29. Kim, J., Forsythe, S. (2008) *Sensory enabling technology acceptance model (se-tam): A multiple-group structural model comparison*. Psychology and Marketing, 25(9): 901-922.

30. Legris P., Ingham J., Collerette P. (2003) *Why do people use information technology? A critical review of the technology acceptance model*. Information and Management, 40(3): 191-204. DOI:10.1016/S0378-7206(01)00143-4.

31. Leite, L., Rocha, C., Kon, F., Milojicic, D., Meirelles, P. (2019) *A Survey of DevOps Concepts and Challenges*. ACM Comput. Surv. 52, 6, Article 127. DOI:10.1145/3359981.

32. Lin, C., Shih, H., Sher, P. (2007) *Integrating technology readiness into technology acceptance: The tram model*. Psychology and Marketing, 24(7): 641-657.

33. Miles, C., (2020) *ITIL 4 and automation - opening up improvement and transformation.*

34. Nixon, J., McGuinness, B. (2013) *Framing the Human Dimension in Cybersecurity*. Transactions on Security and Safety. 13. e2. DOI:10.4108/trans.sesa.01-06.2013.e2.

35. Parasuraman, R., Sheridan, T. B., Wickens, C. D., (2000) *A model for types and levels of human interactions with automation.* IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans, 30: 286-297.

36. Pew, R. W., Mavor, A. S. (2007) *Human-System Integration in the System Development Process:* A New Look. Washington, DC: National Academies Press.

37. Save, L., Feuerberg, B., (2012) *Designing human-automation interactions: a new level of automation taxonomy*. In: De Waard D, Brookhuis K, Dehais F, Wickert C, Röttger Manzey, D., Biede, S., Reuzeau, F., Terrier, P. (2007) Human Factors: A View from Integrative Perspective. Proc. HFES Europe Chapter Conference, Toulouse: p. 43-55.

38. Schepers, J., Wetzels, M. (2007) *A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects*. Information and Management, 44(1): 90-103.

39. Sheridan, T. B., (1992) *Telerobotics. Automation and Human Supervisory Control*. MIT Press.

40. Sheridan, T. B., Verplank, W., (1978) *Human and Computer Control of Undersea Teleoperators. Man-Machine Systems Laboratory*, Dept. of Mechanical Engineering, MIT, Cambridge, MA.

41. Symons, S., France, M., Bell, J., Bennett, W. (2006) *Linking Knowledge and Skills to Mission Essential Competency-Based Syllabus Development for Distributed Mission Operations.* Air Force Research Laboratory, Report AFRL-HE-AZ-TR-2006-0041.

42. Venkatesh, V., Brown, S. (2001) *A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges*. MIS Quarterly, 25(1): 71-102.

43. Vevera A.V., Albescu A.R. (2018) *Factorul uman vs. securitatea cibernetică*, Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, Vol. 28, No. 4, 67-74,

44. Wilding, R., (2007) *Insiders are the biggest enemy*, Strategic Risk.

**Aurelian BUZDUGAN** holds a Master's degree in Software Engineering from the Faculty of Mathematics and Informatics, Moldova State University. Currently he is a doctoral candidate in Computer Programming at the Doctoral School for Mathematics and Information Sciences, Moldova State University. The subject of his doctoral thesis is Decision Support Systems for Minimizing Cyber Risks in Critical Infrastructures. His research interests are cyber security, critical infrastructures, decision support systems and artificial intelligence. He holds international certifications in cyber security such as GCIH, GCFE, CEH, ENSA as well as other areas such as ITIL or Prince2.

**Aurelian BUZDUGAN** a obținut titlul de Master in Științe Exacte in Ingineria Produselor Software de la Facultatea de Matematică și Informatică, Universitatea de Stat din Moldova. În prezent este doctorand la specialitatea Programarea Calculatoarelor la Școala Doctorală de Matematică și Științe ale Informației, Universitatea de Stat din Moldova. Tema programului de doctorat este Sisteme support decizionale pentru minimizarea riscurilor cibernetice în infrastructuri critice. Interesele sale de cercetare sunt securitatea cibernetică, infrastructurile critice, sisteme suport decizionale și inteligența artificială. Deține certificări internaționale în domeniul securității cibernetice, cum ar fi GCIH, GCFE, CEH, ENSA, precum și în alte domenii, cum ar fi ITIL sau Prince2.

**Gheorghe CĂPĂȚÂNĂ, University Professor, Doctor of Engineering**. Graduate of the Faculty of Mathematics and Cybernetics (State University of Chisinau, 1970), Doctor of Engineering (Polytechnic University, Bucharest, 1995), holder of positions: computer scientist (Institute of Mathematics and Computer Science, Academy of Sciences of Moldova); Head of laboratory, Head of department (Union Academy of Agricultural Sciences (ВАСХНИЛ), at the same time, member of the Section "Problem Oriented Complexes", Council of Main Builders, Intergovernmental Commission for the Computing Technique of Socialist States); main specialist (Higher Attestation Commission of the Republic of Moldova); Dean (Cooperative-Commercial University of Moldova), simultaneously, two years of studies, associate professor at the "George Bacovia" University of Bacau; Head of the department "Programming Technologies", State University of Moldova, etc.

He has developed and implemented information systems for enterprises in the Food Industry of Moldova and the USSR, Chisinau City Hall, the Goverment of the Republic of Moldova, the Academy of Sciences of Moldova, the Higher Attestation Commission, the Ministry of Health, etc.

He has over 100 publications, and has trained 8 doctors of science, under direct supervision or co-supervision. He is also an expert of the National Agency for Quality Assurance in Education and Research.

**Gheorghe CĂPĂȚÂNĂ, profesor universitar, doctor inginer**. Absolvent al Facultății de Matematică și Cibernetică (Universitatea de Stat din Chișinău, 1970), doctor inginer (Universitatea Politehnica, București, 1995), deținător al funcțiilor: informatician (Institutul de Matematică și Informatică, Academia de Științe a Moldovei); șef laborator, șef departament (Academia Unională de Științe Agricole (ВАСХНИЛ), concomitent, membru al Secției „Complexe Orientate pe Probleme”, Consiliul Constructorilor Principali, Comisia Interguvernamentală pentru Tehnica de Calcul a Statelor Socialiste); specialist principal (Comisia Superioară de Atestare a Republicii Moldova); decan (Universitatea Cooperatist-Comercială de Moldova), concomitent, doi ani de studii, conferențiar universitar invitat la Universitatea „George Bacovia” din Bacău; șef catedră „Tehnologii de Programare”, Universitatea de Stat din Moldova, ș.a.

A elaborat și implementat sisteme informaționale pentru întreprinderi din Industria Alimentară a Moldovei și URSS, Primăria Chișinău, Conducerea Republicii Moldova, Academia de Științe a Moldovei, Comisia Superioară de Atestare, Ministerul Sănătății, etc.

Are peste 100 de publicații, și a pregătit 8 doctori în științe, personal și în cotutelă. De asemenea este expert al Agenției Naționale de Asigurare a Calității în Educație și Cercetare.