Journal of the International Society for the Systems Sciences | 67th Meeting of the International Society for the Systems Sciences
J.M. Wilby, Editor.

BEING HUMAN IN AN IT ENVIRONMENT

Lynette Drevin
North-West University
Lynette.Drevin@nwu.ac.za

Abstract
In this paper, the reflection will be on different perspectives of humans living in an Information technology (IT) environment. The paper is based on work done by the researcher over many years in IT-related fields; looking back, seeing what is current and looking forward. Rapid change and emergence, complexity of systems, failed and challenged information systems, information and computer (in)security, lack of awareness and training (inter alia), all have an impact on being human in an IT environment. The problem statement that will be investigated is: "There is a lack of coherent knowledge of what is impacting the human living in the IT environment". Humans manage their situation within the IT environment in silos and from their own perspectives. This topic is also being studied and addressed in a somewhat narrow, one-sided way, namely from own contexts. Rapid change within IT systems/software and platforms is not adequately adopted and incorporated by humans to understand how new/adapted systems operate and how to interact securely with these changes. There is thus a need is to ascertain what aspects have an influence on being human in the IT world in order to understand it and interact with it in a safe, holistic manner. The research methodology will be a critical systems thinking approach, where holism and emergence are of importance. The method applied will be a critical reflection of the aspects impacting the human living in the IT environment from different perspectives. Kant asked the three questions about reason: "What can I know?" "What must I do?" and "What may I hope?" These questions will lead this reflective paper, considering different perspectives when addressing the problem statement. The "what can I know" question will focus on several IT-related issues, such as information systems failures and challenges and the possible reasons of this, information security awareness, educational efforts to improve knowledge and skills when interacting with (using and developing) IT systems, and how to understand and incorporate the emergence and rapid change in the IT environment. The "what must I do" question will concentrate on the human's role, e.g., as researcher, subject chair, software developer, engaging in professional societies etc. The "what may I hope" question will focus on how to bring about a better future for humans to cope with and to be living in the IT environment, based on insights and actions (know and do). This is the rationale of this paper – to reflect on how humans can be empowered (involved and affected) to live, work and flourish in the IT environment with all these challenges.

Keywords
Human, IT environment, emergence, failure in systems, information security, education, perspectives, interaction, stakeholders

1 | Introduction

Humans are constantly being exposed to change and must adapt and make sense of new emergences. An overarching reality of these changes is the growing use of Information Systems (IS) within the bigger Information Technology (IT) environment. We cannot even think about transactions and activities where computers and computerized systems do not play a role in our lives. The way that we as humans are impacted by IS and IT has been studied over many years by researchers and other stakeholders (e.g., researchers, academics, and those developing and managing IT projects). These studies are mostly conducted from the contexts and (sometimes narrow) perspectives of these stakeholders, and not from the viewpoints of all the involved or affected parties of these systems Many Information Systems are also are perceived as challenged or failed systems, because they do not meet the expectations of users, or they are not completed within the allocated timeframe and budget (Open Door Technology, 2021).

With the increasing use of IT systems, humans have also been exposed to cybersecurity incidents and they are being affected negatively when they lose money, are being hacked, or sensitive information is being misused. There is a lack in awareness of many of these IT-related issues and people try to make sense from this in their own

way and in silos. Many studies have been conducted on how users can interact in a secure way with IS and how to raise awareness (Aldawood & Geoff, 2019). However, humans still fall prey to cyber-related security incidents.

Abovementioned issues (and many more) all impact the human living in an IT environment. Therefore, the problem statement that will be investigated in this paper is: "There is a lack of coherent knowledge of what is impacting the human living in the IT environment". There is thus a need to ascertain what aspects have an influence on being human in the IT world to understand it and interact with it in a safe, holistic manner and to be able to adapt to this emergent field. This report adopts a critical systems thinking approach, emphasizing the importance of holism[1] and emergence. By reflecting on different perspectives, this paper seeks to answer Immanuel Kant's three fundamental questions: "What can I know?" "What must I do?" and "What may I hope?" These questions (Kant, 1781) serve as a framework for examining various aspects related to the problem statement, considering different stakeholders' perspectives.

The purpose/rationale of the paper is therefore to demonstrate that the affected can be empowered and awareness can be raised about the way in which they interact with IT systems by studying these issues in a multiple perspective and holistic way. The researcher's (author's) publications and studies over many years are also used in an attempt to address the problem in a reflective way.

The structure of the paper is as follows: In section 2, relevant literature background is discussed regarding the IT environment. The research methodology and approaches are provided in section 3. The critical reflection, the main topic of this paper, is presented in section 4. The paper is concluded in section 5, highlighting the three Kantian questions.

2 | Understanding the IT environment (Literature)

This section is used to present an overview of IT-related topics that are impacting the way that humans interact with information systems and displaying challenges they face when they use computerized systems.

2.1 | Information systems failures and challenges

We are surrounded by information systems (IS) in practically every walk of life, and we find it impossible to imagine life without them. In the majority of societal spheres and levels, IS support fundamental operations in fields, such as science, business, medicine, entertainment and education. Additionally, IS increase a company's competitiveness and support the ongoing change that occurs in business and its surroundings. Literature frequently discusses information systems that fall short or are abandoned across a wide range of industries and nations. Users frequently perceive IS as being underwhelming, not living up to expectations, and not providing customers with value. Studies and research have been conducted over many years to identify failure and success factors in order to reduce or eliminate IS failures. Post-project evaluations are frequently utilized to gain knowledge after software projects have been completed, to learn from mistakes and not to repeat these mistakes again.

IS failures are also referred to in the following terms; challenged systems, runaways, disasters, death march projects or development failures. Failures are often seen as software projects that were compromised in one or more of the following (Yourdon: 2004, Ewusi-Mensah 2003, Standish 2001, Glass: 1998):

- Stakeholder expectations and needs about functionality or usability were not met.
- Budget and/or time restrictions were not sustained.
- Poorer than anticipated quality of the end product.

A few examples of failures/or challenged systems/disasters are presented.

1. *London Ambulance service system: UK, 1992:*

Why did London Ambulance Service fail? The system failed to handle the burden that regular use placed on it; it took several hours to respond to emergency calls; ambulance communications broke down, and ambulances disappeared from the system. Regarding developing issues - the system's acquisition, design, and implementation involved a series of mistakes.

2. *"22 people wrongly arrested in Australia due to failures in new NZ $54.5 million courts computer system", 2011*

[1] "Today, *holistic* and *wholistic* are sometimes used interchangeably. *Holistic*, however, is far more common in academic and medical writing. Having *whole* as a base, *wholistic* is often used by writers wanting to emphasize the entirety of something". Source (https://www.merriam-webster.com/wordplay/wholistic-word-origin-and-use).

22 people were wrongfully arrested as a result of 3 600 errors in the electronic transfer of data between the courts to the law enforcement databases. This was due to a new NZ $54.5 million computer system connecting New South Wales courts and accepting documents to be settled in an electronic way.

3. eNaTIS (Electronic National Administration Traffic Information System): South Africa, 2007

There are several reasons why the eNaTIS system failed, but the absence of systematic planning by all parties involved in the project, including the project manager, was the primary one. The project failed as a result of the project scope being altered frequently and new specifications being introduced. Lack of testing, poor project management, and unrealistic expectations for a new system that would completely replace an existing system led to the eNaTIS system failure (Makasi, (2016).

Challenger Disaster NASA 1986

On 28 January 1986, the space shuttle Challenger was engulfed in flames 73 seconds after liftoff. Seven astronauts lost their lives. After investigating the cause of the disaster, it was found that there was "*a serious flaw in the decision-making process leading up to the launch." "Why did NASA push for the launch? It seems the answers have to do with both publicity and politics*" (Veliz, 2021).

IS failures span across many domains and are experienced globally (Drevin, 2014). Despite all that is known about failures and challenges – it still happens.

2.1.1 | **Rapid Technological Change and Emergence**

Apart from technology, including IT, that is changing worldwide in a rapid way, the way software is designed and developed also needs to adapt. Rather than being rigid, flexibility is needed because the systems development process is not a logical process; it is a dynamic process. The process is changing, whether it is changing requirements, changing methodology, changing technology or changing people. As a result, change is a natural, unavoidable part of systems development (Moyo, 2022). So, the human needs to adapt in this changing environment, with new and updated systems and IT equipment and devices. More and more areas of human existence become intertwined with IT, e.g., IoT (Internet of Things). People are using smart phones, social media, doing financial transactions, medical applications, etc. with the incorporation of IT. However, this is not all happening seamlessly – many people struggle and make errors in the process of using IT applications and systems.

2.1.2 | **Complexity of IT Systems**

Literature reporting on IS project outcomes very often lists factors for success and failures (Standish, 2001). Factors that contribute to failures range from systems complexity, poorly defined objectives and unclear requirements to project size, poor communication (between all stakeholders, such as project members and users), and lack of professionalism in reporting.

We live, exist and work within a networked world and these networks form intricate interconnections across space and time in a complex way. This highlights the complexity within organizations processes must be done and transactions need to be performed. Complexity, interconnections, global and social disorder, and systems that are out of balance are just a few of the challenges researchers face when developing and managing IT systems that have to support human actions and transactions (Urry, 2003).

2.1.3 | **Multiple Perspectives**

In order to try and make sense from IT failures, the complexity in systems and the interaction of humans within the IT environment, it is necessary to include multiple stakeholders and their perspectives. In a study done about IS failures where narrative methods were used to understand the situation, a recommendation was listed as: "*Listen and talk to all the stakeholder groups to elicit a collective requirement set for new systems – even though their views may be multi-voiced. All perspectives must be incorporated"* (Drevin, 2014).

By using narrative approaches or storytelling while endeavouring to make sense of IS failures, it was observed that the stories of the stakeholders – although in many instances incoherent and multi-plotted - led to a richer picture and better understanding of the situation A combined research approach was used by Bartis and Mitev (2008) involving narrative methods to study a failed IS. In this study, it was found that all perspectives need to be considered, as the official story is often not the only story. Marginalized voices must also be heard.

2.2 | Information Security and Awareness

With the increased use of computers and online applications, more and more people fall prey to different types of cyberattack, such as social engineering – where phishing and responding to spam emails happen frequently – mostly by unaware users. These attacks become increasingly sophisticated and do not look suspicious.

The Internet of Things (IoT) has seen exponential growth in use in recent years, and with it, so have cybersecurity issues and uneducated users. Artificial intelligence (AI) is at the forefront of cybersecurity and is used to create sophisticated algorithms that shield and secure networks and systems, including Internet of Things (IoT) devices. However, cybersecurity attacks are also on the rise as cybercriminals have learned how to abuse AI (Kuzlu, Fair & Guler, 2021). Users need to be made aware of the variety of current and new cyber risks to help cultivate an understanding of these vulnerabilities in order to act and behave in a more secure way.

3 | Methodology

In this section, the methodological approach taken for this paper, including critical systems thinking, and the introduction of Kant's questions on reason are presented.

3.1 | Critical Systems Thinking Approach

In his chapter *"Messy Issues, Worldviews and Systemic Competencies"*, Bawden (2010) shared his thoughts about critical learning systems at an Australian educational institution. A set of five beliefs that are also of importance for this paper was presented:

- Experience is important in how people learn and develop.
- The learning that takes place is multi-dimensional in that everything around us is shaping our sensemaking.
- Our worldviews influence and filter the way we are learning and how we make sense.
- Worldviews and perspectives may develop as we reflect and use higher order cognitive processing.
- There is a wholeness and inter-connectedness when acting systemically in the world, in order to learn and to make sense.

Thus – in order to understand humans living and interacting in the IT environment, we need to take into account these assumptions when studying such phenomena (IS failures, cybersecurity issues, rapid change, complexity, etc.) in order to try and understand and make sense.

Hammond (2017) presented a basic systems research framework with four cycles, namely observation, reflection, planning and action. She showed that there was a need to acknowledge that fragmented discipline-based research had to emerge in a more integrated approach. The focus had to be broadened and more voices had to be heard. It becomes problematic when problems/issues under investigation are isolated and the focus remains narrow. More components of a system and their interrelationship and the system's relationship with its environment need to be part of the study/inquiry. The researcher's own role and influence in the situation must be recognized, as true objectivity is difficult and reflexive self-awareness is needed. Feedback processes and learning are also important to achieve sensemaking. Thus – to practise or do research according to a systems approach, Hammond (2017) considers and understands the following.

- Interrelationships
- Multiple perspectives
- Boundaries

Reynolds and Holwell (2020) stated that the messy situations and disasters in life involve many interrelated and interdependent factors, and there is so much embedded uncertainty and complexity. Using systems approaches may simplify the way we try to understand or investigate these (often uncertain) situations. In doing so, and using multiple perspectives, underlying issues (not seen in an obvious ways) may be revealed. The concepts of holism and emergence are highlighted, and the complex dynamics of a situation/problem/system, and interaction of the parts/subsystems come to the fore. When applying a non-systems approach, the issues of reductionism (not acknowledging the interconnectedness) and dogmatism (using a single perspective) will be inevitable.

3.2 | Thoughts on reflection and inquiry

"Critical systems thinking (CST) is about critical systems practice. That is, it stands or falls by the ability to promote reflective professional practice"(Ulrich, 2003). Churchman (1968) identifies five basic elements/characteristics when referring to a system:

- Overall objective: the performance measures of the whole system - these cannot be compromised.
- System's environment: Those elements that do not form part of the system but have an impact on the system – also when they change.
- Resources of the system: inside the system, these are under the control of the system, and help achieve the objectives.
- Components of the system: subsystems working together to achieve the main objective.

- Management of the system: coordination of components, setting goals, allocating resources, and controlling the system's performance.

When investigating or studying a problematic/phenomenon, these elements of a system can be used by the researcher or practice to reflect on the situation at hand as guidelines. To add to the richness of reflection/investigation, the commitments of critical systems thinking (CST) of Jackson (1991) are important for improving the situation:

- Critical awareness: be aware of strengths, weaknesses and foundations of techniques, and methodologies.
- Social awareness: think about the consequences when using methods and guide intervention.
- Pluralism – methods and theory level: Use methodologies, methods and perspectives from several traditions or disciplines and contribute to the theoretical level of the discipline.
- Individual emancipation: Empower and facilitate development of individuals to reach their potential.

Ison (2017) uses a picture of a juggler handling four balls for effective practice, namely being a practitioner, with own tradition of understanding, engaging in a real-world situation. Furthermore, the practitioner is busy contextualising and managing his/her involvement in the situation. This focus is on the awareness of the practitioner when involved and engaging in complex and uncertain situations. The aspects listed in this section are used when problematic situations are studied and reflection is done during and after the investigation or inquiry.

3.3 | Kant

Immanuel Kant, one of the most influential philosophers in history, posed three fundamental questions that have continued to guide philosophical and ethical discourse over time: "What can I know?" "What must I do?" and "What may I hope?" In today's rapidly evolving world of Information Technology and the increased interaction of humans with IT, these questions gain new significance as we navigate the complexities of situations such as system failures, lack of information security awareness, and the need for educational efforts to reflect on the challenges posed by the digital era on humanity. The application of the Kantian questions is demonstrated as appropriate and suitable in this digital era in which we are living. Van der Linde and Goede (2021) mapped the work of Kant to using action research for improving programming skills of students.

These aspects on methodological concerns are applied and taken into account when reflection is done on the human in the IT environment. In the next section, a reflection on the problem statement: "There is a lack of coherent knowledge of what is impacting the human living in the IT environment" is presented, using a systems approach and taking into account the methodological topics discussed in this section.

4 | Application of the reflection

The three Kantian questions will be reflected upon indicating how they are mapped/linked to the research done relating to the human living in the IT environment.

4.1 | What Can I Know?

In this section consideration is given to the "*what can I know*" question. It is important to explore IT-related issues and gain a deeper understanding of the interaction between humans and IT systems.

In the realm of information technology, the question of knowledge becomes particularly critical. As technology advances at an unprecedented pace, we are bombarded with vast amounts of information, often making it difficult to discern what is reliable and what is not. System failures and security breaches further erode our trust in the digital landscape. Kant's emphasis on reason and rationality becomes relevant here. We (practitioners, researchers, computer users, etc.) must strive to acquire knowledge through critical thinking and objective analysis. By questioning the sources (including all stakeholders), verifying information, and fostering a culture of skepticism, using a variety of methods from several disciplines, we can navigate the unstable waters of misinformation and make informed decisions.

4.2 | What Must I Do?

Human roles in the IT environment are discussed to address the second question of "*what must I do*". The rapid advancement of information technology has brought with it ethical dilemmas and societal responsibilities that demand our attention. In the face of system failures and vulnerabilities, we must ask ourselves what actions we are obligated to take. Kant's moral philosophy, rooted in the concept of duty and universal moral principles, provides valuable guidance. We have a responsibility to ensure the security and privacy of information, both for ourselves and others. By adhering to ethical principles, such as honesty, transparency, and respect for others' rights, we can contribute to a more trustworthy and reliable information technology environment.

Moreover, the question of what we must do extends beyond individual actions. Institutions, governments, and corporations must recognize their role in safeguarding information and ensuring the responsible use of technology. By implementing robust security measures, promoting awareness campaigns, and enforcing legal frameworks, we can create a collective commitment to information security and mitigate the risks posed by rapid technological advancements. However, in all this, all stakeholders' perspectives, interaction between subsystems and awareness of one's actions should be considered.

4.3 | Previous studies conducted mapped to "What can I Know" and "What can I Do"

In an attempt to comprehend what we can learn from IS failures/challenges/software development/security concerns/educational efforts etc., a few studies and analyses in which the author was involved are used for reflection. Exhibit 1 is used to provide the title, the area in which knowledge was/is gained and how this was/or could be applied in doing. Other reflective comments are also given on methods and perspectives.

Exhibit 1. Examples of research studies: mapping the "Know" and "Do" questions

Study	What can I know?	What can I do?	Comments
Towards the Development of a Contingent Use of Systems Development Methodologies Model (Moyo et al., 2022)	Improved systems development practices. Assist researchers to investigate the contingent use of Software Development Methodologies (SDM) and improve their implementation in systems development projects.	Apply improved SDM and practices – software developers. Educate IT students regarding these improved practices, raise awareness	Empirical study and findings. Theory and practice evolve and inform one another. Developers', users', managers', and researcher's perspectives
Deep Learning Affective Computing to Elicit Sentiment Towards Information Security Policies (Du Toit et al., 2022)	People can give fake answers when asking their opinion – e.g., on security issues. To address response bias, this study used computerized methods to perform sentiment analysis, based on facial expressions. Decision makers can be provided with a tool and methodology to evaluate the quality of their Information Security Policies.	Use a variety of approaches when decision makers want to get more accurate opinions.	Proposed a deep learning affective computing approach to perform sentiment analysis, based on facial expressions. Staff, managers', and researcher's perspectives
Anomaly detection using autoencoders with network analysis features (Ball et al., 2023)	Identifying fraudulent /anomalous activities in financial ecosystems. Expressing the interactions between participants in a system as a mathematical graph allows researchers to apply social network analysis (SNA) to understand the nature of these relationships better.	Use of autoencoder to detect anomalies in a transactional setting.	Unified approach: neural architecture, autoencoder model, threshold optimization process, Gaussian scaling. Staff, managers', and researcher's perspectives
Incorporating various perspectives in using instant messages in teaching programming: A critical system thinking perspective (Manduna et al., 2022)	How can we teach programming using Instant Messaging (low cost, accessible tool), as a Learning Managing Systems (LMS) with proper theoretical underpinning?	Applying the IM tool as alternative compared to more sophisticated LSM, in order to give more students access to programming education.	Critical systems heuristics was used as a multi-methodological framework, incorporating various conditioned realities. Lecturers', students', researcher's perspectives
IT students' awareness of the negative effects of	People can often become victims of technology abuse and cybercrime, and then they are not equipped to counteract the	A mobile app was developed to educate users regarding these concerns. Awareness and training	A survey was conducted - observations in a classroom and electronic questionnaires were

technology (Drevin & Kim, 2019)	negative effects of technology. Aspects or the dark side of technology entails all the negative side-effects of technology, such as plagiarism, information security threats, technostress, etc.	programs are needed for students who are not adequately educated about the dark side of technology, otherwise there is the possibility that information technology users may become victims of cybercrimes and scams. In doing so graduate attributes, such as "responsible and engaged members of society" and others are addressed.	used. Lecturer's, students', and researcher's perspectives
Children's Awareness of Digital Wellness: A Serious Games Approach (Allers et al., 2021)	Children are vulnerable and need protection. Children learn – by playing and also using books and games. Games can aid in raising awareness in the digital space.	Using a mobile serious game to promote digital wellness among pre-school children	Educational games, expert reviews, experience, and feedback. Teachers', parents', and researcher's perspectives
Key elements of an information security culture in organisations (Nel & Drevin, 2019)	A list of 21 unique security culture elements was identified from the literature. The list was enhanced after input from practitioners.	Organizations can use the framework of information security culture aspects to ensure that an organization incorporates all key features in its own information security culture. Use of the framework may lead to improved security awareness and safer cyber security behavior of employees.	Literature reviews with the focus on: security culture and information security. Analysis and comparison of these studies were done. Construction of a framework. Survey conducted in which respondents were asked to assess the importance of the elements and to record possible missing elements/aspects regarding their organizations' information security culture to construct an enhanced framework. Staff, users', managers', and researcher's perspectives
Student and manager perspectives on the graduate attributes of IT students after Work-integrated Learning (WIL) (Redelinghuys & Drevin, 2019)	Gain insight into and compare the perspectives of students and employers on the graduate attributes of IT students when they did Work-integrated Learning (WIL)	With the insight gained in this study, lecturers can address shortcomings in the curriculum. Address enhancement of work readiness and other graduate attributes, such as communication, planning time management, integrity	Survey – quantitative and qualitative data collected. Content analysis. Multi-perspectives taken into account. Interaction between educational efforts and industry studied. Students', employers', managers', and researchers' perspectives
Learning from Information Systems failures by using narrative and antenarrative methods (Dalcher & Drevin, 2003), Making sense of information systems failures (Drevin, 2014)	Gain insight into IS failures. What are success and failure factors? Studies are mostly done post-fact and in silos - multi-perspectives often to be considered. Using stories from different stakeholders can give richer insight into the messy and subjective narratives.	Problematic situations and failures call for a new repertoire of methods to address the unique features of failures. Borrow from other disciplines, e.g., narrative analysis.	Case histories to gain insight into failure. Narrative analysis, content analysis, multiple perspectives, listen between the lines to what is said. Give a voice to the marginalized. Looking back, what is currently going on, improper / incoherent storytelling, and what will follow? Interaction between stakeholders, the system and environment. Developers', users on different levels', managers', software companies and researcher's perspectives

4.3.1 | Knowing

It is important to understand and know the reasons behind shortcomings in IT systems to study/research and investigate the IT environment that has an impact on humans. The above table lists topics, such as software development practices, failures, complexity, rapid change in IT and how to adapt, cyber security concerns, information security issues and awareness and educational (SoTL) research.

4.3.2 | Doing

Furthermore, after understanding (and knowing) these issues, we need to get to doing. As individuals and users of systems, we have a duty to adapt and continuously update our skills to keep pace with technological advancements. Equally important is the collective responsibility of all stakeholders, organizations, and educational institutions to provide opportunities for lifelong learning and reskilling, ensuring that no one is left behind in this fast-changing landscape.

The author – as educator and researcher had (still has) several contributions and responsibilities over time regarding these topics.

a) The research completed as seen in Exhibit 1 as examples of studies conducted.
b) Post graduate students' supervision also in the above-listed topics.
c) Subject Chair (line management) in the academic institution.
d) Educator.
e) Engaging in professional societies.

The first two in the list (a) and (b) and (d) are handled in the table in Exhibit 1, indicating the know and do questions. During the research process of the studies, the aspects of CST were taken cognizance of, namely the overall objective of the system, the environment, the resources of the system, the subsystems and the management of the system and coordination of all components. To revisit the commitments of CST as earlier stated (Jackson, 1991), all aspects (a-e), but especially the other roles of the author (c), (d) and (e) can be reflected upon in the following ways:

- Critical awareness: How to provide supervision? Which research methods to use? How to approach stakeholders in studies? Which teaching and learning strategies to employ? Engaging staff and empowering and supporting them/guiding them to handle (and flourish in) their T&L situations.
- Social awareness: Will the stakeholders be happy and use the new system? Will the user interface work for them in accordance with the companies' procedures? Will requirements be met? Will the solution work in the origination and culture? Will the problems be solved? Will the users be empowered to solve own problems and adjust to new situations? Will the system work in the environment? What about outside influences (out of the researcher's control)?
- Pluralism - methods: Can methods from other disciplines be used – e.g., Failure investigation borrowed methods from social sciences, namely narrative analysis and sensemaking with stories. Multiple perspectives of stakeholders were crucial in sensemaking.
- Individual emancipation: Educational efforts may lead to empowered students. By raising awareness in the information security field, users may act more secure and not be susceptible to cyberattacks – the human still remains the weakest link where cyberthreats are concerned (Knowbe4, 2023). To deploy improved system development methodologies, better software can be developed. Are staff members in control of their situations? As member/chair of discipline societies, can other members be encouraged and see hope/get innovative ideas for T&L or research? This last commitment of emancipation especially implies hope, which is addressed in the next section.

4.4 | What May I Hope?

The "*what may I hope"* question is considered in this section where we can reflect on creating a better future for humans interacting with the IT environment. In an ever-changing information technology landscape, it is essential to maintain a sense of hope and optimism. Kant's question regarding hope invites us to consider the possibilities that lie ahead. Despite the challenges we face, technology also offers great potential for positive change. Educational efforts play a vital role in shaping the human experience in this environment. By incorporating software development skills, information security awareness, digital literacy, and ethical considerations into curricula, we can equip individuals with the tools they need to navigate the digital world confidently and with professionalism.

Additionally, emerging technologies, such as artificial intelligence (AI), IoT, automation and others, hold promise for enhancing security and improving efficiency. By embracing these advancements responsibly and

ethically, we can build a future where information technology empowers individuals, works securely, fosters innovation, and contributes to societal well-being. Exhibit 2 presents the mapping with "what may I hope".

Exhibit 2. Research studies mapping the "What May I Hope" question.

Study	What may I hope?
Towards the Development of a Contingent Use of Systems Development Methodologies Model (Moyo et al., 2022)	Improved and more effective software development practices, addressing all stakeholder needs. Improved interaction between the IT environment, and companies where these systems are being used
Deep Learning Affective Computing to Elicit Sentiment Towards Information Security Policies (Du Toit et al., 2022)	More honest feedback from users when interacting with security policies to provide their feedback. Provide an opportunity for openness and discussion between management and staff. Empowerment of all stakeholders.
Anomaly detection using autoencoders with network analysis features (Ball et al., 2023)	Minimizing fraud in financial transactions. Better data integrity in the systems, improved service delivery to clients.
Incorporating various perspectives in using instant messages in teaching programming: A critical system thinking perspective (Manduna et al., 2022)	Give access to more learners (including students) to education in the discipline of computer programming. Emancipation of the marginalized.
IT students' awareness of the negative effects of technology (Drevin & Kim, 2019)	Students reflect on their online practices by engaging in the survey. Students become more aware of the dangers of the digital realm, and learn to interact in a more secure way, and in doing so, become more responsible cyber-users.
Children's Awareness of Digital Wellness: A Serious Games Approach (Allers et al., 2021)	Raise children with more awareness of cyberthreats, in the safe environment with their parents, in a fun way. In doing so the parents are also becoming more educated and sensitive to what their children are doing online and can warn them about the consequences.
Key elements of an information security culture in organisations (Nel & Drevin, 2019)	Improved security practices in companies and among staff. The focus is also on non-technical issues where political and organizational cultures are some of the concerns.
Student and manager perspectives on the graduate attributes of IT students after Work-integrated Learning (WIL) (Redelinghuys & Drevin, 2019)	We may hope for improving the development of graduate attributes in students by letting them engage in industries when doing WIL. Feedback from employers gives valuable insight to the lecturers and students. Students also reflecting on their own activities and learning experiences, letting them develop into true academic scholars.
Learning from Information Systems failures by using narrative and antenarrative methods (Dalcher & Drevin, 2003) Making sense of information systems failures (Drevin, 2014)	Improved information systems to address the needs of users of all levels. Better interaction between stakeholder groups – e.g., developers and users. Reflecting on lessons learned when developing systems as not to repeat the same errors. Being sensitive to all stakeholders' perspectives, subsystems, the environment and complexities we may hope for systems improving humans' lives, transactions, and overall integration with IT.

Hopefully, with these types of study and activity, insights are gained, and lessons learned, e.g., in software development practices, the way failures are investigated and analyzed, we then may hope that all involved will play an active role to practice responsible engagement with IT. The value of considering multiple perspectives can be seen and using methods from other disciplines for enrichment and deeper understanding, are appreciated. The empowerment and emancipation of students and other people affected (often the marginalized) is seen. Education plays a crucial role in shaping the future of technology and therefore the curriculum must also stay abreast in the fast-changing world.

5 | Conclusions

Immanuel Kant's three fundamental questions provide a valuable framework for addressing the challenges posed by IT-related problematic situations, such as systems failures, lack of information security awareness, rapid change in information technology, complexity in systems, and the need for educational efforts to study and address these concerns. By striving for knowledge, engaging in these situations, and embracing hope, we can navigate the interactions and complexities of the information technology environment and shape a future where technology can be used as a very important tool in support of many human applications. As individuals (researchers, practitioners, computer users) and as a society, we must remain aware, continuously reflecting on our actions and responsibilities to ensure a harmonious integration of humanity and technology. With this reflection the problem statement of the paper is addressed: There is a lack of coherent knowledge of what is impacting the human living in the IT environment and using reflective and systems approaches, better insight and understanding are achieved.

As we are trying to cope and live with problematic issues in the IT environment, we must continually examine what we can know, what we must do, and what we may hope for in this digital age. By asking these questions, reflecting, using multiple perspectives for understanding, looking at the parts and the whole of a situation (and system), we can strive to build a technologically advanced world that we as humans will be able to comprehend, and with which we are able to engage in an ethical way. In doing so, individuals/the affected and society become empowered and are able to navigate the complexities of the digital landscape with wisdom, integrity and hope.

6 | References

Aldawood, H., & Geoff, S. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. *Future Internet Journal*, *11*(73). https://doi.org/10.3390/fi11030073

Allers J., Drevin G.R., Snyman D.P., Kruger H.A., & Drevin L. (2021). Children's Awareness of Digital Wellness: A Serious Games Approach. In: Drevin L., Miloslavskaya N., Leung W.S., Von Solms S. (eds) Information Security Education for Cyber Resilience. WISE 2021. *IFIP Advances in Information and Communication Technology*, vol 615. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-80865-5_7

Ball, R., Kruger, H., & Drevin, L. (2023). Anomaly detection using autoencoders with network analysis features. *ORiON*, 39(1). https://doi.org/10.5784/39-1-711

Bawden, R. (2010). *Messy issues, worldviews and systemic competencies*. Chapter 6 in Blackmore, Chris (ed). 2010. Social Learning Systems and Communities of Practice. https://doi.org/10.1007/978-1-84996-133-2_6

Churchman, C.W. (1968). *The systems approach*. New York: Delacorte Press.

Dalcher, D., & Drevin, L. (2003). Learning from Information Systems failures by using narrative and antenarrative methods. (In Eloff, J., Kotze, P., Engelbrecht, A. & Eloff, M. eds. IT Research in development countries. *Proceedings of SAICSIT 2003*: South Africa: A Volume in the ACM international conference proceedings series). https://hdl.handle.net/10520/EJC27968

Drevin, L. (2014). *Making sense of information systems failures*, (Doctoral thesis, Middlesex University, UK). https://eprints.mdx.ac.uk/14410/

Drevin, L., & Kim, J. (2019). IT students' awareness of the negative effects of technology. *Conference proceedings of the 10th International ISTE conference on Mathematics, Science and Technology Education*, South Africa. http://hdl.handle.net/10500/26085

Du Toit, T., Kruger, H., Drevin, L., & Maree, N. (2022). Deep Learning Affective Computing to Elicit Sentiment Towards Information Security Policies. *Advances in Science, Technology and Engineering Systems Journal*, *7*(3), 152-160. https://www.mdpi.com/1424-8220/21/15/5135

Ewusi-Mensah, K. (2003). *Software development failures: anatomy of abandoned projects*. London, England: MIT Press.

Hammond, D. (2017). Philosophical foundations of systems research. A guide to systems research: *Philosophy, processes and practice*, 1-19. https://link.springer.com/chapter/10.1007/978-981-10-0263-2_1

Ison, R. (2017). *Systems practice: How to act: In situations of uncertainty and complexity in a climate-change world*. London: Springer London. https://link.springer.com/book/10.1007/978-1-4471-7351-9

Jackson, M. C. (1991). The origins and nature of critical systems thinking. *Systems practice*, *4*, 131-149. https://link.springer.com/article/10.1007/BF01068246

Kant, I. (1781). *Critique of pure reason* (translated and edited by Paul Guyer & Allen W. Wood). Cambridge: University Press.

Knowbe4 (2023). *Report: Phishing By Industry Benchmarking*. https://info.knowbe4.com/phishing-by-industry-benchmarking-report

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*, 1-14. https://link.springer.com/article/10.1007/s43926-020-00001-4

Makasi, F. (2016). *eNaTIS What Went Wrong, From a Project Manager's View*. https://www.linkedin.com/pulse/enatis-what-went-wrong-from-project-managers-view-fulela-makasi/

Manduna, W., Goede, R., & Drevin, L. (2022). Incorporating various perspectives in using instant messages in teaching programming: A critical system thinking perspective. *Systems Research and Behavioral Science*, *39*(5), 947-961. https://doi.org/10.1002/sres.2893

Moyo, B., Huisman, M., & Drevin, L. (2022). Towards the Development of a Contingent Use of Systems Development Methodologies Model. In: Insfran, et al. (Eds) *Advances in Information Systems Development. Lecture Notes in Information Systems and Organisation*, vol 55. Springer, Cham. https://doi.org/10.1007/978-3-030-95354-6_16 ISBN: 978-3-030-95354-6

Nel, F. & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and Computer Security*, 27(2) pp. 146-164. https://doi.org/10.1108/ICS-12-2016-0095.

Redelinghuys, M. & Drevin, L. (2019). Student and manager perspectives on the graduate attributes of IT students after Work-integrated Learning (WIL*). Conference proceedings of the 10th International ISTE conference on Mathematics, Science and Technology Education*, Kruger National Park, Mpumalanga, South Africa, 21-25 October 2019. Pretoria: UNISA. ISBN 978-1-77615-062-5. http://hdl.handle.net/10500/26102

Reynolds, M., & Holwell, S. (2020). *Introducing systems approaches. Systems approaches to making change: A practical guide*, 1-24. https://www.amazon.com/Systems-Approaches-Making-Change-Practical/dp/1447174712

Standish. (2001). *Extreme Chaos*. http://www.standishgroup.com/sample_research/PDFpages/extreme_chaos.pdf.

Ulrich, W. (2000). Reflective practice in the civil society: the contribution of critically systemic thinking. *Reflective practice*, *1*(2), 247-268. https://doi.org/10.1080/713693151

Ulrich, W. (2003). Beyond methodology choice: critical systems thinking as critically systemic discourse. *Journal of the Operational Research Society*, *54*, 325-342. https://www.jstor.org/stable/4101702

Urry, J. (2003). *Global Complexity*. UK: Polity Press. https://www.jstor.org/stable/3186411

Van der Linde, S., & Goede, R. (2021). From Kant's Critique of Pure Reason, to Action Research in Improving the Programming Skills of Students. *Systemic Practice and Action Research*, *34*(4), 419-440. https://link.springer.com/article/10.1007/s11213-020-09543-8

Veliz, L (2021). *How the challenger space shuttle explosion could've been avoided*. https://www.grunge.com/595986/how-the-challenger-space-shuttle-explosion-couldve-been-avoided/

Yourdon, E. (2004). *Death March*. Upper Saddle River, NJ.: Prentice Hall. https://books.google.co.za/books/about/Death_March.html?id=FdAZUX9H_gAC&redir_esc=y