Insight into User Acceptance and Adoption of Autonomous Systems in Mission Critical Environments

Article *in* International Journal of Human-Computer Interaction · June 2022

DOI: 10.1080/10447318.2022.2086033

7 authors, including:

Kristin Weger
University of Alabama in Huntsville
27 PUBLICATIONS **31** CITATIONS
SEE PROFILE

Lisa Matsuyama
University of Alabama in Huntsville
4 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Bryan Mesmer
University of Alabama in Huntsville
60 PUBLICATIONS **249** CITATIONS
SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
106 PUBLICATIONS **456** CITATIONS
SEE PROFILE

International Journal of Human–Computer Interaction

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/hihc20

Insight into User Acceptance and Adoption of Autonomous Systems in Mission Critical Environments

Kristin Weger, Lisa Matsuyama, Rileigh Zimmermann, Bryan Mesmer, Douglas Van Bossuyt, Robert Semmens & Casey Eaton

To cite this article: Kristin Weger, Lisa Matsuyama, Rileigh Zimmermann, Bryan Mesmer, Douglas Van Bossuyt, Robert Semmens & Casey Eaton (2022): Insight into User Acceptance and Adoption of Autonomous Systems in Mission Critical Environments, International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2022.2086033

To link to this article: https://doi.org/10.1080/10447318.2022.2086033

INTERNATIONAL JOURNAL OF HUMAN-COMPUTER INTERACTION
https://doi.org/10.1080/10447318.2022.2086033

Taylor & Francis
Taylor & Francis Group

Insight into User Acceptance and Adoption of Autonomous Systems in Mission Critical Environments

Kristin Weger[a], Lisa Matsuyama[a], Rileigh Zimmermann[b], Bryan Mesmer[b], Douglas Van Bossuyt[c], Robert Semmens[c], and Casey Eaton[b]

[a]Psychology, The University of Alabama in Huntsville, Huntsville, AL, USA; [b]Industrial and Systems Engineering and Engineering Management, The University of Alabama in Huntsville, Huntsville, AL, USA; [c]Systems Engineering, The Naval Postgraduate School, Monterey, CA, USA

ABSTRACT
With Industry 4.0 the immense progression of Artificial Intelligence (AI) technology has introduced new challenges for engineers to effectively design human-automation interaction in autonomous systems that are mission critical. Although various autonomous systems are currently being utilized in mission critical environments, there is limited literature and research on which factors affect the acceptance and adoption of said systems. Understanding which factors are most critical for the human-automation interaction could lead to seamless acceptance and adoption and more effective and less expensive missions. Findings of 47 semi-structured interviews revealed ease of use and system reliability to be significant factors for the acceptance and adoption of autonomous systems independent of the level of automation. Through our findings we expand on the current technology acceptance models by including mission critical factors. Emphasis is given to the discussion and consideration of the human factors and engineering approaches associated with the design of autonomous systems for mission critical environments that are needed to empower tomorrow's users with effective AI systems technology.

1. Introduction

Many agree that a good use of a robot is for tasks that are dirty, dangerous, or dull, and war has plenty of these tasks. As such, the military has a very strong interest in system autonomy and human-autonomy teaming, especially in mission critical environments (Barrett-Pink et al., 2019). Current and future mission environments are dynamic and opaque wherein interactions and their related consequences become increasingly more complex to isolate and comprehend. With the growing capacity and ubiquity of autonomous systems, the human-automation interaction has become the center of attention for disciplines such as human factors psychology, computer science, and systems engineering to develop systems that ensure human-automation viability (Ghazizadeh et al., 2012). Yet, systems intended for use in mission critical environments, such as for military operations, have often been built without engineers being aware of user's preferences, values and consequences for the human-automation interaction when defining system requirements.

As autonomous system performance becomes progressively more dependent on the integrity of the relationship between the human and the autonomous system, the human factors associated with autonomous systems use becomes critical. For example, an user's role may change as they adopt a new autonomous system versus an older system that was only partially autonomous or required full manual user input to function (e.g., calculating and entering parameters). Instead of remaining in complete decision-making control of the operation, an autonomous system may require users to allocate control of the mission operation to the system itself (e.g., Shneiderman, 2020). Because of the dependability in the human-automation interaction with users being contingent on systems with various levels of autonomy, acceptance and adoption of such systems by users is critical to mission success and the viability of future systems (Hutchins & Hook, 2017).

The aim of this research is to present unique insight into currently serving military personnel's views on the existing and future state of automated systems and factors surrounding their acceptance and adoption. Identifying factors by military end-user that attribute to the acceptance and adoption of these systems informs current technology acceptance models, and future system design requirements and processes. Moreover, the generated understanding may have a substantial impact on the field's understanding of system use and design for military applications.

CONTACT Kristin Weger kw0004@uah.edu Psychology, The University of Alabama in Huntsville, 1310 Ben Graves Drive, Morton Hall, Room 208, Huntsville, AL 35899, USA

1.1. Mission critical autonomous systems

In civilian applications, a mission critical system can refer to a system that is essential to the survival of an organization and will adversely affect society when it fails (Hinchey & Coyle, 2010). Within the U.S. military, mission critical refers to any job functions that are identified as critical to the performance of the agency (Meyer, 2020). An example of a mission critical system in a military context is the navigational system for a spacecraft. If the navigational system were to fail, the spacecraft would either have degraded performance or could be lost entirely. Many mission critical systems can have major adverse impacts with the possibilities of loss of life, serious injury and/or financial loss if they fail especially in unanticipated ways. Within systems, specific components or subsystems can be mission critical where a failure of the component or subsystem causes the system to no longer function as anticipated which can cause hardware failure, software failure, or a loss of trust in the system by the user. Hence, the acceptance and adoption of mission critical autonomous systems is essential to improve military efficiency and safety because of an increase in system and mission complexity as well as a decrease in overall manpower in the military (Barrett-Pink et al., 2019; Benaskeur et al., 2011).

Within mission critical environments, definitions of an autonomous system are not congruous which leaves much room for interpretation. Hence, this study uses the definition provided by the North Atlantic Treaty Organization (NATO; Taddeo & Blanchard, 2021) to describe autonomous systems. According to NATO, an autonomous system within the military can be defined as "a system that decides and acts to accomplish desired goals, within defined parameters, based on acquired knowledge and an evolving situational awareness, following an optimal but potentially unpredictable course of action," (Taddeo & Blanchard, 2021). These systems can range from simple autonomous systems such as a handheld Global Positioning System (GPS) device to complex autonomous systems such as drones for which the human-automation interaction can vary in complexity. Based on the U.S. Department of Defense Task Force Report (2012) the overall goal for the use of autonomous systems is to extend and improve human capability while the human remains in the decision-making loop or the Observe-Orient-Decide-Act (OODA) Loop (Maccuish, 2012; Ryan & Mittal, 2019).

Current design and development of autonomous systems for military use have shown limited system adaptability to users' expertise and roles that run the risk of interfering or diminishing the user's capability (Militello & Klein, 2013), in the form of diminished manual skills (Cunningham & Regan, 2015) or loss of situation awareness (i.e., human out of the loop phenomenon; Endsley & Kiris, 1995). Moreover, automated systems designed for mission critical environments have been found to provide more capabilities than users can comprehend or use (Strauch, 2017) that may result in increased user workload or "automation surprises" if the automated system performs unexpectedly (Kaber et al., 2006; Sarter et al., 1997). Therefore, the system design has a direct influence on users' willingness to accept and adopt it, and as such, understanding the various factors that affect acceptance and adoption is essential for advancing autonomous system design.

1.2. Acceptance of autonomous systems

For many years, researchers have applied theories of human behavior, like trust in automation, to study technology acceptance and adoption (Hoff & Bashir, 2015). While current literature is convoluted with an interchangeable use of both terms, it is important to draw on theory to understand the differences between the term acceptance and adoption of autonomous systems.

Acceptance has been defined as an attitude towards an autonomous system, and is influenced by various factors, such as perceived usefulness, ease of use, level of automation, perceived user control, and prior automation exposure (Bekier et al., 2012; Davis, 1985). Indeed, a user who has a new automated system available for use, has not yet adopted it because there are additional stages beyond the availability of a system where acceptance plays an important role. For instance, experienced warfighters, military personnel, may believe that in combat, the less-capable system that works 100% of the time is preferred over the new, but unreliable autonomous system. Thus, even if a user has a new autonomous system available to them but does not accept it, adoption is unlikely to occur (Renaud & Van Biljon, 2008). Hence, the acceptance of a technology can begin long before the user has first contact with the system (Ekman et al., 2018).

Literature on determinants that affect early acceptance show that the acceptance of a system is affected by the level of automation and the control the user has. For instance, air traffic controllers' acceptance of automated decision-making systems decreases as the level of automation increases with complete rejection of such a system when decision-making is completely removed from the user (Bekier et al., 2012). On the other hand, research suggests that automation that takes over mundane tasks to be more accepted by users as it allows users to stay cognitively engaged in other more challenging tasks (Bekier et al., 2012). Prior exposure to automation seems to alter user acceptance, particularly then when system automation conforms to the way the user thinks, ultimately leading to increased acceptance (Hilburn et al., 2014). Therefore, acceptance of technology has been found to be an essential step along the way for adoption to occur (Matsuyama et al., 2021).

1.3. Adoption of autonomous systems

Adoption is a process that starts with the user becoming aware of the technology and ending with the user embracing the autonomous system by making full use of it (Davis, 1985). Autonomous systems can be adopted or rejected by either individual users or by the entire social system, which is dependent on the level of decision power given to the user for adopting an autonomous system. Adoption is influenced by factors such as word by mouth, reviews, and actions by others (Hinz et al., 2014), with negative reviews leading to late adoption (Jahanmir & Cavadas, 2018). Moreover, research indicates beliefs of increased control and flexibility (i.e., optimism), confidence or proficiency in technology, dependency and feeling of vulnerability during the interaction with the system (Ratchford & Barnhart, 2012), and trust (Choi & Ji, 2015; Kaur & Rampersad, 2018) to be essential for adoption to occur.

Research on determinants that affect early adoption shows that adoption is affected by attitude towards that system, tendency to adopt technology early, and benefit from solving user needs (Jahanmir & Cavadas, 2018). Technology adoption has been referenced to a life cycle, which suggests that every new technology innovation is accepted by individuals at different rates (Moore, 2002; Rogers, 2003). Individuals have been defined as being either innovators, early adopters, early majority, later majority, or laggards. For instance, innovators are eager to adopt innovations even if it means that they must work hard to make these innovations work for them. On the other hand, the early adopters, who comprise one third of the market are strongly driven by practicality with well-established references that the technology is stable; while the late majority, also one third of the market prefer to wait until the product is an established standard with significant support. Thus, it is suggested that adoption of an autonomous system can only occur once a user is completely invested in the system and begins to make full use of its capabilities (Matsuyama et al., 2021).

1.4. Technology acceptance models

The use of models to estimate technology acceptance and adoption is not novel and past models have presented an effective way to investigate use cases and nuisance criteria for system development purposes (Hutchins & Hook, 2017). One widely used model for technology acceptance is the Technology Acceptance Model (TAM; Davis 1989). TAM was developed on the concept that individuals accept or reject technology based on the perceived usefulness and perceived ease of use of that technology. The goal of TAM is to provide an explanation of the determinants of computer acceptance that is general, capable of explaining user behavior across a broad range of end user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified.

Besides TAM, more complex models of acceptance such as Technology Acceptance Model 2 (TAM2), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the Safety-Critical Technology Acceptance Model (SCTAM) have been released with the intent of improving the models used in gaining more accurate information on acceptance of technology across disciplines (Hutchins & Hook, 2017). For instance, the UTAUT suggests differently than the TAM, that variables such as effort expectancy, performance expectancy, and social influence by user influence their intention of accepting a system (Taiwo & Downe, 2013). However, the major limitation of current models is the basis of design with current technology acceptance models being based on user-focused technology (e.g., information systems or computers). These types of systems are inherently safer than the autonomous systems used in military missions like an autonomous weapon system. Thus, the technology acceptance models may not encompass the context of technology use in complex and mission critical environments, such as the use in battlefields. This poses the opportunity to evaluate possible mission critical determinants and extend the model with such attributes.

While extensive literature and research supports the theories surrounding the acceptance and adoption of commercial systems, the literature surrounding mission critical autonomous systems, such as military systems, is rather limited. Thus, in order to advance system requirements and system design of mission critical systems it is of importance to better understand the various factors surrounding system acceptance and adoption. Thus, this paper presents unique insights from current serving military personnel through exploring factors related to the acceptance and adoption of current autonomous system and future autonomous system developments to progress. Further, findings of this research aim to inform existing technology acceptance models in literature (Davis, 1989) to better capture autonomous systems operationally used in mission critical environments. Therefore, this research addresses three main research questions:

> Research Question 1: What is the view on the current and future role of autonomous systems in mission critical environments?
>
> Research Question 2: How does personnel view the acceptance and adoption of current autonomous systems in mission critical environments?
>
> Research Question 3: What factors should system designers consider during the development of new autonomous systems to improve user acceptance and adoption?

It remains imperative to answer these questions, given the increased role of AI in the human-automation interaction and the impact that interaction has on mission capability, survivability, and operations success.

2. Method

To investigate the factors that users find essential toward the acceptance and adoption of autonomous systems, a semi-structured interview was conducted. Users were the target participants to elicit domain knowledge as subject matter experts (SMEs) in the field of mission critical autonomous systems. In addition, participants were asked which factors would change their trust, result in complete rejection of autonomous systems and which factors need to be considered in future system design.

2.1. Participants

Forty-seven active-duty military officers and students enrolled in the Naval Postgraduate School (NPS) participated in this study. Of the 47 participants ($n = 43$ males), 23

Table 1. Examples of SME area of operation, job roles and systems used in daily operation.

Example areas of operation	Example job roles	Example systems used in daily operation
Cyber operations/information systems	Combat engineer	Radar/Infrared/Alert systems
Engineering/science	Communications officer	Software programs for mission-, safety-, cyber-critical applications
Infantry	Cyber-operations officer	Unmanned Aerial Vehicle
Logistics	Engineer	Tactical systems
Specialized combat forces	Field artillery officer	Weapons systems
	Infantry soldier	
	Infantry officer	
	Logistic officer	
	Pilot	
	Special operations forces	
	Simulation operation officer	
	Submarine officer	
	Warfare officer	

Note. SME: subject matter expert.

Table 2. Qualitative interview questions and word count breakdown of question responses provided by participants.

#	Example question	Word count mean	Word count range
1	What was your background before coming to NPS?	43	6–132
3	What is an autonomous system to you?	77	7–1190
4	In your opinion, what is the level of automation of the system that you used in your military career?	39	1–344
5	What were the autonomous systems that you used and how did they aid in your operations?	126	6–1070
8	Describe your level of acceptance for that system	82	1–651
9	What might lead to change in your trust in that system?	101	9–372
10	What might lead to complete rejection of the system that you work with?	58	3–279
11	What was good about the system that you used that made it easy to accept and adopt?	77	13–201
12	What challenges did you encounter with the autonomous system that could lead future users to not accept or adopt the system?	118	11–721
13	What factors for the use of autonomous systems are essential for you to want to accept and adopt an autonomous system?	106	3–475
14	In your opinion, do you see autonomous systems having a role in future military operations?	21	1–195
15	Where do you see such systems having the most benefit and why?	152	37–815
16	What do you think needs to be addressed in future design and development of autonomous systems for users to accept and adopt them more readily?	139	8–654
17	How would you change the training on future autonomous systems for users to accept and adopt them?	139	9–530
18	Have you ever been consulted in the development of new autonomous systems prior to their release and operational use?	21	1–195
19	What are your views on the consultation of current and future personnel during the design and development phase of new autonomous systems?	173	4–1839

were from the United States Marine Corps, 12 from the Navy, 7 from the Army, 5 from the Air Force and Coast Guard.

Number of years of service ranged from 4 years to 17 years, on average SMEs had 11 years of Experience and were considered mid-career officers. All participants were older than 18 years of age. Table 1 presents a selection of the area of the SME's roles and systems used in daily operation. Due to the complex nature of the environment, military officers have experienced a rise in the use of automated and semi-automated systems to support their day-to-day working.

In regards to the operational use of various levels of automation of a system, respondents indicated the level of automation of the systems they used. To the vast majority, participants ($n = 23$) indicated to use partially autonomous systems, that still needed human interaction, but minimal to none (i.e., input parameters). Multi-level autonomous systems were used by 12 participants which had various levels of autonomy per system with varying amounts of human interaction. Ten participants indicated to use complete autonomous systems that did not need human assistance. Two respondents indicated to use decision- making support systems that made decisions on their own. A full breakdown of time in position, all the previous and current job roles, systems used in daily operations is not provided due to the number, sensitivity, and specificity of answers.

2.2. Materials and procedure

Data were collected through interviews with participants. The interview was semi-structed and consisted of 19 open-ended questions that asked about participant's experience with an autonomous system, as well as factors surrounding the nature of acceptance and adoption of the system. Questions and response examples are provided in Table 2. Questions were based on extensive literature research and expanded prior research of the British Royal Navy (Barrett-Pink et al., 2019). The questions were reviewed by SMEs from the Naval Postgraduate School (NPS) and the interview process was pilot tested to ensure understandability and reliability. The questions were developed to capture what factors are essential for the acceptance and adoption to effectively operate in the relationship between users and the autonomous system. Participants took between 30 and 40 min to complete the interview.

After responding to an invitation to participate in the study, participants were emailed a consent form and date and time for their Zoom interview session. With the start of the interview, participants were asked if they agreed with the consent form, and if they consented to being audio recorded for transcription purposes. Participants then indicated their background and experience with the autonomous system before being asked about factors regarding the acceptance and adoption and finished with their views on the consultation of current and future personnel during the design and development phase of new autonomous systems. Following the completion of the interview, participants were debriefed and thanked. The study was approved by the University Institutional Review Board (IRB) and in compliance with applicable Department of Defense and Department of the Navy human research protection policy. Chi-square analyses were run with SPSS.

2.3. Interview coding analysis

Interviews were recorded as audio files; therefore, the first stage of analysis was to transcribe the audio file into Word documents. Dragon software (Baker, 1975), which is a commonly used speech recognition technology that converts spoken word into written text, was utilized to facilitate the transcription process. Given the data sensitive nature, the dragon software was licensed to an independent computer station and data was saved to the local hard drive for further analysis.

For analyzing the structure interview questions inductive content analysis, a qualitative method of content analysis, was utilized to identify themes in the transcribed data (Elo & Kyngäs, 2008; Kyngäs et al., 2020; Schamber, 2000). Inductive content analysis is an approach which utilizes an inductive starting point where data collection is open and follows loosely defined themes (Kyngäs et al., 2020). If rigorously applied, this analysis technique can provide an insightful method of analysis for research questions as themes and ideas emerge inductively from the data. Inductive content analysis was chosen over other qualitative methods (e.g., thematic analysis) and methodologies (e.g., grounded theory) as it is a structured analysis method that has been found to be useful for producing analyses suited to informing conclusions. Inductive content analysis was used as a research method to make replicable and valid inferences from the data, with the purpose of providing information, new insights, and a practical guide to action.

A crucial consideration for conducting inductive content analysis is the transparency of the approach taken, which can affect upon the validity of the findings. Guidelines produced by Kyngäs and colleagues were followed to ensure a robust approach to thematic analysis occurred. With inductive content analysis, codes are built and developed by initially reviewing data points and then grouping recurring statements, conversation topics, and expression of feelings or opinions into categories based on notes taken on the data. Once data is reviewed and notes are evaluated, a set of codes, or a coding scheme, is determined to be used to categorize data points. This process is differentiated from deductive content analysis, where a predetermined set of categories is used to group data points into like categories. When reviewing these inductively derived codes alone, the context may seem meaningless; however, when these codes are combined within a coding scheme, it is possible to view a comprehensive picture of the area under exploration. Following the initial generation of content categories, the data were reread to review each category against the coded items and the entire data set, making the analysis iterative in nature. Once the categories for the codes were generated from the data and reviewed, existing literature and documentation available to the author were interwoven into the findings to facilitate comprehension of the results. In general, a five-step procedure was used to (1) identify data, (2) determining coding categories, (3) code the content, (4) check validity and reliability, and (5) analyze the results. This allowed for a holistic overview of the collective experience of autonomous systems by participants and the promotion of ecological validity of our research results.

3. Results

The interview data of 47 participants were used for qualitative analyses. Two coders separately reviewed a total of 73,378 words with an average response length of 79 words that were generated by participants for all questions during the interview. Refer to Table 2 to review word count breakdown per question. Coders identified codes for common factors participants expressed across the different questions. After the initial coding, coders consolidated and simplified the codes through code validation. The raters then formulated a general description of each code as seen in Table 3. Quotes presented throughout the result section are taken directly from SME responses to allow the reader to judge the veracity of the underlying themes that emerged. Where text was intentionally removed, "[…]" will symbolize the omitted words.

3.1. Interrater reliability

Interrater reliability (IRR) was calculated by the number of agreed upon codes for all questions. Cohen's Kappa was used as the analysis of IRR because it determines the level of agreement between primary and secondary coders. It is commonly cited that kappa statistics of 0.00–0.20 to indicate slight agreement, 0.21–0.40 to indicate fair agreement, 0.41–0.60 to indicate moderate agreement, 0.61–0.80 to indicate substantial agreement, and 0.81–1.00 to indicate almost perfect agreement (Landis & Koch, 1977). IRR was computed for how the raters agreed on coding. Raters coded data points with both primary and secondary codes, with primary codes being considered the more prominent code

Table 3. Main coding themes, definitions, frequency and IRR.

	Themes	Description	Frequency	IRR
Factors	Perceived Ease of Use	How easy it is to learn to use, and/or use the system	79	κ =.80, $p < 0.05$, 95% CI [.64, .96]
	Reliability	Proof that the system works repeatedly, accurately, and does not need a lot of maintenance/is resilient	78	κ =.86, $p < 0.05$, 95% CI [.73, .99]
	Perceived Usefulness	When the new system can offer better capabilities or replace an old system, better physical and software attributes- including interoperability	66	κ =.88, $p < 0.05$, 95% CI [.76, 1]
	Human in the Loop	A human intervention component, especially in decision-making	34	κ =.88, $p < 0.05$, 95% CI [.74, 1]
	Transparency	Understanding the intricacies of the system and why users need the system	31	κ =.72, $p < 0.05$, 95% CI [.46, .98]
	Safety/Security	Hardware and software safety (not easy to hack, physically resilient system)	28	κ =.92, $p < 0.05$, 95% CI [.80, 1]
	System Effectiveness	The system saves time, money, manpower	13	$\kappa = 1$, $p < 0.05$, 95% CI [1, 1]
	Interoperability	The system is able to be easily integrated into current and future systems	13	κ =.88, $p < 0.05$, 95% CI [.64, 1]
	Data Error	The system makes mistakes based on sensor, machine or human input	12	κ =.72, $p < 0.05$, 95% CI [.32, 1]
	Customization	The system is better designed than the current system	7	$\kappa = 1$, p = .157, 95% CI [1, 1]

Note. These codes and descriptions represent main factors. CI: confidence interval.

Table 4. A selection of quotes to support the definition of autonomous systems

Example	Quote
1	Autonomous system is a system that can act and decide for itself based on the guidance given to it by its paired user.
2	A purely autonomous system […] is capable of understanding an environment and defining and developing the best rules to make a plan within that environment to meet an objective it is preprogrammed to do […] the ability to choose between different choices to meet the objective.
3	Is a system that operates with little to no input from a human operator making much of its own decisions.
4	Performing some of the functions that ordinarily require a person to do within certain boundaries on their own. So in varying degrees whether it's entirely without human action or within some set boundaries. So things like human on the loop or in the loop, I still consider autonomous if they perform some function that I would usually have performed on my own
5	An autonomous system is a system that works on its own based on a certain set of rules, or accomplishes a task that was previously done by people with some kind of control.

of the two. Interrater reliability was calculated for both primary codes and secondary codes and an overall kappa rating for each main coding theme was determined by averaging both kappa ratings. Interrater reliability, significance levels, and confidence intervals for each main coding theme are provided within Table 3.

There was substantial agreement between the two raters (κ = .895, $p < 0.0005$, with 95% confidence intervals [.87, .92]). After IRR was determined, in a final step, coders discussed any responses for which there was disagreement on their codes.

3.2. Use of autonomous systems in mission critical environments

A total of 4,120 words emerged from the data when exploring Research Questions 1. In order to ground our results in the understanding by the SME's of what an autonomous system is, respondents' definitions were compared for similarity. Our results identified the perception of what an "autonomous system" is to be to 95.74% consistent among SME's ($N = 47$); see Table 4. SME's described an autonomous system as a system that is designed to carry out decisions and processes with minimal input or oversight from an actual user. Respondents also stated that they not only use one definition for autonomous systems instead specifically define the level of automation when referencing a certain system. In addition, more than half of respondents defined autonomous systems by stating that human operators must have the ability to intervene in system control loops and to assume manual control when needed (i.e., human-in-the-loop). This corresponds to the U.S. Department of Defense statement that the overall goal for the use of autonomous systems is to extend and improve human capability while the human remains in the decision-making loop (Maccuish, 2012; Ryan & Mittal, 2019).

SME identified currently used operational systems across domains covered by RN operations; radar, tactical systems, unmanned aerial vehicles, etc. Table 1 displays examples of the systems identified. Further SME's indicated the level of automation of the current system used during operation. To the vast majority, respondents ($n = 23$) indicated to use partially autonomous systems, that still needed human interaction, but minimal to none (i.e., needed input parameters from the user). Multi-level autonomous systems were used by 12 personnel which had various levels of autonomy per system with varying amounts of human interaction. Ten respondents indicated to use complete autonomous systems that did not need human assistance. Two respondents indicated to use decision-making support systems that made decisions on their own.

In line with prior research (Barrett-Pink et al., 2019), automated systems across military domains were identified to support tactical decision making by facilitating the fusion

Table 5. Future area of application and description for autonomous systems in military environments.

Areas		Description
Application	Mundane tasks	The system greatly increases the efficiency of doing everyday tasks or the system handles these tasks themselves automatically which allows human users to focus elsewhere on more significant decisions
	Big data analytics	The process of uncovering trends, patterns, and correlations in large amounts of raw data to help make data-informed decisions.
	Tracking/early warning systems	The system is used to track targets' locations, advances, aggressions, etc. (and potentially allow us to counter those threats, such as early warning systems, missile tracking, etc.)
	Logistics	The system will benefit logistics of materials, people, or machinery
	Drones/unmanned aircraft	Autonomous systems are best utilized through drones or other unmanned aircraft
	Cyber areas	The system helps combat cyber/computer-related areas (such as hacking and cyber-attacks)
	Dangerous situations	The system replaces manpower in potentially dangerous/lethal situations
	Finance/business	The autonomous system is used to handle calculating finances/business processes

of sensor data and providing the user with direct access to the information needed to make informed decisions.

> Immediately it is tactical systems that can make decisions on their own. Whether that's drones that have a targeting system on there, systems that have a battle buddy or a unit on the battlefield. […] long-term, systems that help with decision making, analyzing all the information that's out there to help make the best decision.

Besides, respondents identified future autonomous systems to benefit greatly logistics and supply chain in order to become more efficient and amplify overall logistical capabilities ($n = 16$). Oher fields of applications for autonomous systems mentioned entailed tracking or early warning systems ($n = 19$), drones and unmanned aircrafts ($n = 14$), cyber areas ($n = 4$), dangerous situations ($n = 3$) and finance/business ($n = 2$), see Table 5.

Moreover, future automated systems were identified to reduce mental workload, particularly for staff functions –who are responsible for the administrative, operational, and logistical needs of a unit. Respondents specifically noted future autonomous systems to increase efficiency and capability across the military by automating mundane tasks ($N = 23$) such as data processing or physical logistic transport. For example, Artificial Intelligence (AI) applications were identified as a promising tool to improve data processing of tracking/early warning systems or drones and unmanned systems to support decision making:

> This unstructured big data needs to be somehow categorized, processed and some analytics needs to be done to them in order for us to be able to figure out what we're looking at and following decisions.
>
> Analyzing all the information that's out there to help make the best decision.

Personnel highlighted that decision making by an autonomous system leaves still many unanswered questions when it comes to the decision-making matrix as it pertains to the rules of engagement. Rules of engagement constitute the legal framework that governs how military personnel can use force. Questions centered around rules of engagement that need to be answered include "When does a human get involved?" "Does a human need to be involved?" "What's the risk of innocent deaths that we're willing to accept vs … appropriate kills?". There is a growing body of literature exploring the ethical considerations of the use of automated systems in mission critical environments to direct policy development (Royal Society for the encouragement of Arts, Manufactures and Commerce [RSA], 2018). The awareness of the ethical questions of using automated systems is reflected by the respondents remaining reticent to hand over complete control of decision making to an automated system.

3.3. Acceptance and adoption of current autonomous systems in mission critical environments

A total of 436 words emerged from the data when exploring Research Questions 2. From the questions discussing the factors associated with the acceptance and adoption of the operational use of current autonomous systems, ten overarching themes emerged. Table 6 provides example quotes for each identified theme.

To get an understanding of whether SME's accepted the current autonomous system used during operation, respondents were asked to rate their level of acceptance. Participants indicated somewhat to accept the system ($n = 17$), almost complete acceptance of the system ($n = 14$), complete acceptance of the system ($n = 11$), and low acceptance of the system ($n = 4$). Respondents attributed "complete acceptance" of the system to factors such as *perceived usefulness, perceived ease of use, reliability, human in the loop, and customization.*

Specific to autonomous systems used within mission critical environments is that respondents would use a system with low capability in place of no system. Such responses demonstrate the circumstances personnel use autonomous systems and the dependability on these systems for decision making during life-or-death scenarios.

> […] my stance is always, and always will be, use everything that you have until it becomes compromised.
>
> […] so we're like "well, it's a program from 1985, but it works", so I guess it's fine.

Beyond, respondents mentioned that supply chain issues associated with the difficulty of getting supply parts quickly when a part of the system breaks is a factor playing into the level of acceptance of the autonomous system by the end-user.

From the question discussing challenges encountered with the autonomous systems six themes emerged, perceived

Table 6. Themes and example responses regarding operational use of autonomous systems.

Themes	Examples
Ease of Use	"How the end user uses it, the ease in which they use it, builds immediate confidence in its ability to perform its function."
Reliability	"[…] if it was throwing up some false positives then there's an issue because it could lead to complacency in users and they just assume everything is okay and won't do the check. So that could be dangerous."
Perceived Usefulness	"It freed up a lot of bandwidth for me and allowed me to focus on other things that were equally or more important than micromanaging whatever the system was."
Human in the Loop	"I've seen a few times where the autopilot does something incredibly wonky or fails to disengage, which isn't normal and most of the time we can override it without much of a problem. But the thing is, even a system that we rely on very heavily, almost like another member of the crew, "George", George still makes mistakes. The problem is when George is given that level of authority over the aircraft and our lives, those mistakes can be costly, and if you have no way of correcting George then that's a big problem."
Transparency	"I also mean by that the transparency of […] especially when it gets into those complex and very complex systems […]."
Safety/Security	"If an autonomous system overrode my inputs in an unsafe manner. That would be it." / "I think if it was shown to have been compromised then that would be a huge reset in not just the implementation of that system […]"
System Effectiveness	"To reduce the workload in the time and human hours that are invested into the same thing or significantly reduce risk."
Interoperability	"If it was able to communicate to other autonomous systems a little better."
Data Error	"If you put left instead of right […], the autonomous output of the solution to avoid the danger would be wrong."
Customization	"It was tailored to our […] work. […] it was built off of like a foundation that had been around for awhile … "

Figure 1. Level of automation by the frequency of encountered challenges on the x-axis.

ease of use (30%, 15 cited by SMEs), interoperability (20%, 10 cited by SMEs), resource constraint (20%, 10 cited by SMEs), reliability (14%, 7 cited by SMEs), mental workload (4%, 8 cited by SMEs), or data error (4%, 8 cited by SMEs). Themes were divided by level of automation for qualitative analysis. Table 6 provides example quotes for each identified theme and Figure 1 provides an overview of themes based on the level of automation.

Interestingly, an additional theme of resource constraint emerged during a secondary qualitative analysis of the responses. Personnel using partially autonomous systems identified the challenges with the current system to be related to resource constraint. A common issue faced by branches is to operate with a decreased budget and number of personnel. Respondents stated the impact it has on employing automated systems in order to maintain operational capability such as no proper training, slow response related to troubleshooting or maintenance of the autonomous system. Beyond "perceived ease of use" of the autonomous system was identified as a challenge for personnel using partially autonomous system.

Personnel using both multi-level and complete autonomous systems stated the system to be challenging because the user interface was not intuitive or user-friendly, with a need for intensive training to understand the complexity of the system (perceived ease of use). In addition, challenges exist in that these systems are not interoperable with other (newer) systems. While there is the existence of individual autonomous systems, to be effective in mission critical environments these systems need to be engineered to work as part of the larger systems of systems they will support once deployed. Hence, with most military missions depending on sets of systems to be effective, unit capability is greatly reduced if an autonomous system is unable to interoperate with other systems in use (Table 7).

From the question discussing changes in trust and complete rejection in an autonomous system eight themes emerged. SME's identified factors of reliability (42,2%, 19 cited by SMEs), perceived usefulness (15.6%, 7 cited by SMEs), safety/security (8.9%, 4 cited by SMEs), human in the loop (8.9%, 4 cited by SMEs), perceived ease of use (6.7%, 3 cited by SMEs), transparency (6.7%, 3 cited by SMEs), data error (6.7%, 3 cited by SMEs), and interoperability (4.4%, 2 cited by SMEs) to change trust in an autonomous system. Note that participants responded to change in trust in form of decline in trust by the user in the autonomous system. Similarly, SMEs identified complete rejection of an autonomous system to be attributed to reliability

Table 7. Example responses from SME's related to current autonomous system challenges.

Theme	Quote
Perceived Ease of Use	"It's not very user friendly, somebody has to really know what they are doing to operate it or it's very easy to get either an incorrect result or no result at all […] So for example, it gave the user the opportunity to enter data into fields where it didn't apply at all."
Interoperability	"The operation procedures we received from the manufacturer […] did not match the version of our system, system of systems we had on board."
Resource Constraints	"So one of the big problems is funding and manning, getting […] [users] actually trained on the system," "the support that comes with […] the contract side in terms of managing the system."
Reliability	"We had some connectivity issues with one of them and at one point," "The reliability of the communications network."
Data Error	"if you have bad data that you're trying to look for, obviously you're not going to find what you're trying to get. So, really, a lot of it depends on what you're given by someone else to try and track down."
Mental Workload	"As that one user has so much going on, he gets tunnel visioned into what's going on in the […] [system], he doesn't even see what's going on around him."

Table 8. Example responses from SME's related to changes in trust and complete rejection of autonomous system.

Theme	Quote
Perceived Ease of Use	"It turns out it's really hard to initialize it properly, put in the right parameters from the beginning. Not user friendly." [Change in Trust] "If there is no user interface to it, so like if there is no way to control or if they are just staring at lines of code … " [Complete Rejection]
Reliability	"If it was throwing up some false positives then there's an issue because it could lead to complacency in users and they just assume everything is okay and not do the check." [Change in Trust] "If the batch updates quit going through […], or if the system just totally got fried." [Complete Rejection]
Perceived Usefulness	"If it doesn't perform up to whatever my personal or institutions expectations are." [Change in Trust] "If it continues to adapt to support the helicopter or people that use it, if it doesn't do that I think it would be easily rejected." [Complete Rejection]
Transparency	"It's the instances when I'm like I don't know how this thing is actually able to function that I am less trusting of it. So, having the background and knowing what the system is doing makes me trust it." [Change in Trust] "Autonomous systems, by design, are hard to understand. The harder they are to understand, the fewer people that will understand them and the more people that don't understand them, it's really easy to see a critical tipping point where you get that critical mass of mistrust." [Complete Rejection]
Security/Safety	"If it becomes more frequent or noticeable that any of these systems are easily broken into." [Change in Trust] "If it was shown to have been compromised then that would be a huge reset in not just the implementation of that system" [Complete Rejection]
Human in the Loop	"As long as there's not a mechanism where it locks us out and we can't do anything unless it detects a problem." [Change in Trust] "Systems […] under that category of having life or death consequences. So, in that case, […], not having a human at least in the loop to give the go ahead, give the thumbs up, would probably be a no-go for me." [Complete Rejection]
Data Error	"That's probably my biggest fear with […] all autonomous systems - if it doesn't have good data inputs you can't really trust what's going on." [Change in Trust] "[For] complex and very complex [systems] I would image integrity-based errors meaning that it's not actually telling us the truth is a pretty significant reason to abandon that system. [Complete Rejection]
Interoperability	"If it was able to communicate to other autonomous systems a little better," "If it isn't able to adapt to future applications." [Change in Trust]
No Rejection	"It's a program of records" [Complete Rejection]

(27,7%, 13 cited by SMEs), perceived usefulness (25.5%, 12 cited by SMEs), safety/security (14.9%, 7 cited by SMEs), human in the loop (14.9%, 7 cited by SMEs), perceived ease of use (2.1%, 1 cited by SMEs), transparency (2.1%, 1 cited by SMEs), data error (2.1%, 1 cited by SMEs), and no rejection (10.6%, 5 cited by SMEs). See Table 8 for representative responses regarding factors affecting change in trust in a system by military personnel.

Respondents identified system reliability followed by perceived usefulness, safety/security, and human in the loop to be leading factors for changing user's trust that could result in complete rejection of the autonomous system for users operating in mission critical environments. Shneiderman (2020) describes a reliable system to support human responsibility and explainability. Respondents highlight the importance of reliability of autonomous systems to ensure appropriate use and in order to facilitate user trust (see also Hoff & Bashir, 2015). Respondents further noted that if information as to why the system error occurred was missing, trust in the reliability of the system declined. To note is that a lack of reliability may lead to complete rejection of the system, while for change in trust, a surplus of reliability may lead to more trust in the system. Additionally, a lack of perceived usefulness, safety/security, and a lack of the option of having a human in the loop were also critical factors that would lead participants to completely reject the system. One interesting result is the response "no rejection." As the SME's were all active-duty military, the "no rejection" response may indicate that in addition to the contractual duty these users hold, any autonomous system is better than no system in a mission critical environment.

3.4. Factors system designers should consider during the development of new autonomous systems to improve user acceptance and adoption

A total of 578 words emerged from the data when exploring Research Questions 3. From the questions discussing the

Table 9. Example responses from SME's related to essential factors in future design of autonomous system.

Theme	Quote
Perceived Ease of Use	"Easy enough to use that I would spend less time doing that then actually doing the task itself" "ease of troubleshoot and ease of user interface" "it's got to be pretty straightforward […]. The user interface of here's all the data, not just say, 'Oh push the button, we're good.' When the UAS picks up the heat signature of four vehicles, it zooms in and compares them, and shows everything that the AI is doing. Then bringing up its samples and everything it says, 'Yes, with 98% accuracy these are these vehicles and here's why."
Reliability	"A verification validation process, knowing the system will behave the way we expect it to behave and that the information we put into it will make it respond in the manners we expect it to."
Perceived Usefulness	"Is it relevant, does it support or add to what our mission is." "make the process of accomplishing whatever our objective is, or whatever the objective of the machine is, a significantly faster or more efficient pace."
Transparency	"Knowing what's going on with the system", "… the workflow, ease of the workflow, being able to follow my inputs to outputs." "the ability to remove the black box of autonomy to understand why it's doing what it's doing"
Security/Safety	"Is it going to be safe for me to use this and not be detected by somebody else" "It's got to be easily usable but it's also got to be secure. So if it's capable of being hacked and turned to either one process bad or put bad outputs out […] that's a big concern."
Training	"you gotta train people on it, what it's doing and why it's doing it." "there's [currently] no field implementation where they come out and show you how to use it in a field environment."

development of new autonomous systems to improve acceptance and adoption for systems used in mission critical environment, eight overarching themes emerged (see Table 9).

Respondents identified factors of perceived ease of use (42.5%, 20 cited by SMEs), system reliability (23.4%, 11 cited by SMEs), perceived usefulness (17%, 8 cited by SMEs), system transparency (12.8%, 6 cited by SMEs) and security/safety (4.3%, 2 cited by SMEs) to be essential factors for increasing the acceptance and adoption of future autonomous systems.

> The user interface needs to be such that it's easy to operate. It needs to have reliability and some means of being able to troubleshoot any errors that come up. Certain levels of consistency and dependability.

Respondents identified perceived ease of use followed by system reliability, and perceived usefulness to be leading factors for essential factors that need to be addressed in future autonomous system design. Personnel did not mention in detail what perceived ease of use meant in regards to the use of the autonomous system they had experience with. However, personnel highlighted the interface design for autonomous system to be intuitive and to design the interaction in a way the user is already familiar with. For instance, to integrate the use of virtual reality systems from the commercial sector to increase the user's ability to employ the system instantaneously and without the necessity for intensive training.

In addition, human-centered design aspects that need to be addressed in future autonomous systems included human in the loop and interoperability. During military operations, the human will always remain in the decision-making loop. Therefore, system design needs to be able to adapt to their users to become increasingly sophisticated systems. Moreover,

Respondent highlighted future systems to be designed with the capability to integrate with other systems more readily, so that users do not have to operate systems independently from each other.

Beyond the different fields of application of future autonomous system and AI technology, participants indicated that training for these systems is still considered crucial. Participants indicated training of future autonomous systems to entail system specific training for users ($n = 12$) with an early introduction to the system in order to build experience ($N = 8$) and through hands on training on the system ($n = 7$). Additionally, participants indicated a need to increase training in form of occurrence and hours ($n = 8$) and to provide generalized training to higher command ($n = 5$). Overall, ease of training ($n = 3$) with the use of diverse training methods ($n = 2$) is preferred. Further, a preference was shown for industry experts or SMEs to conduct portions of the systems-centered training ($n = 2$). Representative responses from participants can be found below.

> I think education, and by education, I mean training. And more hands-on use of the specific systems, techniques, tactics, and procedures that the systems will use, for the end user, will greatly increase it, and specifically there needs to be more education and instruction and information to the decision makers. It's great that all the […] [users] know how to use this […] automated system […]. If the commander who's making the tactical decisions […] is not educated on the proper use and implementation of those systems because he lacks the first-hand knowledge, and this will go up as decision makers are higher up the chain of command, then […] [the autonomous system] won't be properly employed and used, and that's where I think we run the risk of potential damages to ourselves […].

> Training, the fact that our […] [users] were trained well on that system is important, because if they're not, A you lose the appreciation of what that system is doing for you and B you lose your understanding of what it's doing for you, so if you have to go fix the system or troubleshoot the system at all and you don't know what it's doing you're not gonna be able to do it. So you have to be able to understand what it's doing.

It has been argued that to design automated systems that individuals understand and, therefore, use effectively, it is important to include as many as possible in the design process. However, results on consultation showed, that only 29% of the 47 total participants interviewed had been consulted during the research and development phase of autonomous systems that were made for military use. Further, 93% of the 43 participants hold a positive view a on consultation of end users, and feel it is necessary to create useful, and easy to use systems to foster effective human-autonomy teaming in mission critical environments. Emerging from the data is a clear desire from current personnel to be consulted in the design and development stages of new automated systems.

4. Discussion

Users are having to interact effectively with autonomous systems in mission critical environments to increase mission capability, survivability, and mission success. As these systems start to evolve and become more complex in nature, it is imperative the field understands what impacts the human-automation interaction. While, previous research has reviewed aspects concerning the acceptance of autonomous systems used in the commercial field (Ghazizadeh et al., 2012; Levy & Green, 2009; Matsuyama et al., 2021), a clear understanding of these surrounding factors for mission critical systems is missing that would guide engineers in developing more impactful autonomous systems for end-users.

Given the significance to practitioners, the aim of the current study was to explore the factors affecting the acceptance and adoption of autonomous systems in mission critical environments according to active-duty military personnel. Specifically, we explored factors regarding the acceptance and adoption of current autonomous systems that held various levels of automation, what factors would lead to change in user trust or complete rejection of a system, and what factors should be considered in future system design. Interview data were collected on participants' subjective experience, beliefs, and preferences regarding their use with partial, multi-level or complete autonomous systems or decision-making systems through a series of open-ended questions.

There was no clear consensus among respondents regarding "one" essential factor for autonomous system acceptance and adoption, which displays the complexity of autonomous system design for human-autonomy teaming in mission critical environments. Instead, respondents displayed a preference for several factors with the most essential being *perceived ease of use* in the human-automation interaction, *reliability* of the system, it's *perceived usefulness* for the task at hand, *transparency* of what the system is doing and how its behaving, as well as the *security/safety* of the autonomous system against internal or external-attacks. These findings were not associated with the level of autonomy, suggesting that these factors apply to all levels of autonomy from partial to complete autonomous systems in mission critical environments.

Respondents also identified factors that would lead to change in trust or complete rejection of the autonomous system during critical operations. Both questions resulted in similar findings with *reliability* and *perceived usefulness* being of greatest concern for a change in user trust and were the leading factors for a complete rejection of the autonomous system. These findings postulate that the level of *reliability* or *perceived usefulness* of an autonomous system influences the amount of trust a user has for that system. For example, a user interacting with an autonomous system that presents erroneous information or failures (i.e., reduced system reliability) leads to lower levels of user trust towards the automation; yet the user may continue to rely on the automation to complete the mission's objective (Chavaillaz et al., 2016). Moreover, our findings propose that if the user reaches the tipping point where he/she defines automation not to be reliable nor useful, then the user will reject further use of that system (Bekier et al., 2012). A distinct difference between these responses to possible civilian responses should be noted, as some officers did state nothing would cause them to completely reject a system if it was assigned to them. Within mission critical environments and life-dependent scenarios, personnel would rather use a system with low capabilities rather than having no system. Other factors that were identified by respondents to change user trust and to lead to complete system rejection were *safety/security*, *human in the loop*, *perceived ease of use* or *data error* among others.

Challenges users acknowledged that may affect novice users to accept or adopt current autonomous system included *perceived ease of use*, *interoperability*, *resource constraints*, *reliability*, *mental workload*, or *data error*. For all levels of automation, *perceived ease of use* of the current systems was identified to be the greatest challenge. Yet, our analysis of the automation level revealed, that users current challenge with partial-autonomous systems includes *resource constraints* (i.e., limited funding, manning, training, system managing support from contract side etc.) and with multi- and complete autonomous systems includes *interoperability* and adaptability issues with other systems. These factors were believed to affect novice user's acceptance and adoption of these autonomous systems, which paves the road for "lessons learned" to design more impactful autonomous systems. Indeed, *perceived ease of use*, *reliability, transparency, interoperability,* and *human in the loop* were identified as human-centered design aspects that based on the respondents need to be addressed in future autonomous systems for mission critical environments.

Our study's findings therefore extend the widely used TAM model to capture the factors associated for autonomous systems used in mission critical autonomous systems. For instance, the TAM identifies Perceived Usefulness and Perceived Ease of Use as impacting the attitude towards use and the intention to use (acceptance), which in turn impact the actual usage (adoption) of the system (Davis, 1989). Our proposed model confirms these and several other attributes from the SCTAM model (Davis, 1989; Hutchins & Hook, 2017). Together with the results from the interview data, this blend of information was applied to propose a technology acceptance model for mission critical environments. This allowed to take in to account the Perceived Ease of Us and Perceived Usefulness of the original model modified by the general beliefs which influence them from the other

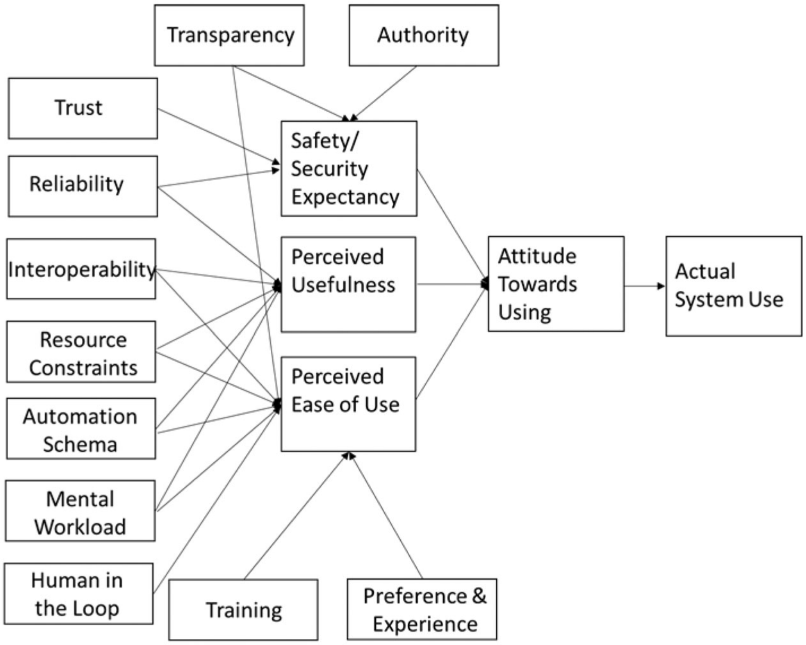

Figure 2. Mission critical technology acceptance model (MCTAM).

variations of TAM such as the SCTAM from the interview information, see Figure 2.

The value of Reliability (R) is defined as the view by adopters of the current state of the autonomous system that incorporates data error, failure rates, perceived failure rate. Trust (T) is described as the trustworthiness of the autonomous system and affected by reliability, safety and security of the system and related to the influences of social norm and authority. Transparency (Tr) is the knowledge of how the autonomous system works, knowing how the system makes its decision and through its feedback greatly impacts the adopters decision-making. Authority (A) represents a determinant to Safety Expectancy (SE). In mission critical context, Authority is the autonomous system having the approval of the governing body over the operational use, in this case the rules of engagement and command and control (this is the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission), which is a binary input but has an impact on how adopters view autonomous systems. In addition, Interoperability (I) and Resource Constraints (RC) were identified as determinants of Perceived Usefulness. Human in the Loop (HIP), Mental Workload (WK), and Training (Ta) were identified as determinants of Perceived Ease of Use.

These findings paint a picture of the complexity surrounding the factors that affect the acceptance and adoption of autonomous systems in mission critical environments. While users seem to show consensus towards a greater emphasis on human-centered design (i.e., ease of use, transparency, etc.) among all levels of automation, system reliability seems to be one of the most imperative factors given its direct impact on users trust and reliance during human-automation interaction in mission critical environments. The study's findings can be leveraged to develop autonomous systems that operate more effectively in the relationship between users and autonomous systems (Barrett-Pink et al., 2019), inform engineering disciplines and design principles (e.g., design specific incentive structures (Flynn et al., 2021)).

5. Implications of findings

Although the autonomous systems were utilized in the military, implications can be transferred to the civilian world. For example, DOD contractors and military organizations are integrating commercial off the shelf (COTS) products in the design of autonomous system. Also, several participants mentioned that perceived ease of use was important in the sense where someone more familiar with a system (like an XBOX controller) would learn on that system much more quickly than if they were given a completely new controller or system that they are not familiar with (see, Hall 2012).

First, while the voice of the users is usually considered in requirements generation and management in system design processes, these percentages show a disconnect between current officers at NPS and the designers of systems they have used in their military career. Several potential sources for this disconnect may factor in; however, data was not collected on why the disconnect is perceived to exist in the respondent population. For instance, maybe these users had not been consulted but others had been. The top essential factors found to have the most impact on the acceptance and adoption of autonomous systems for users could also guide engineers and designers in the development and presentation of current and future autonomous systems for mission critical environments. Another potential take-away from this research is the need for users to feel like they have buy-in on autonomous system development processes, so they are more accepting of autonomous systems in general. It may also help to improve requirements generation and requirements fulfillment throughout the system design process to have significantly more users (e.g., warfighters) involved.

Second, the results of this work align with ongoing work around zero-trust systems engineering for autonomous systems (Hale et al., 2021; Papakonstantinou et al., 2019, 2020, 2021; Van Bossuyt et al., in press). A significant issue facing mission critical autonomous systems is the potential for threats from personnel both internal and external to the system lifecycle from the very earliest parts of system architecture and requirements generation through to design, manufacture, operation, upgrade and maintenance, and eventual disposal. This research has shown that trust in autonomous systems and autonomous systems that are reliable are both very important to users, particularly to warfighters operating in mission critical environments. The zero-trust paradigm in systems engineering aims to produce more reliable and more trustworthy systems through not trusting anyone or anything involved with the system. This often means increased redundancy and diversity in all aspects of the system. Information from this article can be used to further guide zero-trust systems engineering to increase the likelihood that new autonomous systems will be adopted more readily by users operating in mission critical environments.

Third, findings in this article can be used to “buy down” risk of autonomous system adoption failure by focusing on the system design process. In our professional experience, many autonomous systems are relegated to dusty warehouses or are discarded at forward operating bases because the warfighters do not trust the systems or do not find the systems to be useful. By using the information in this article to inform system requirements development and management, engineers may be able to reduce such issues thus reducing overall cost to the taxpayer. Designing and manufacturing autonomous systems that the user trusts and finds useful reduces the costs associated with scrapped systems or major system upgrades required to convince users to trust and adopt autonomous systems.

From a model-based systems engineering (MBSE) perspective and digital twin (DT), the results of this study can be used to improve the models that represent autonomous system end-users. The factors identified in the study are essentially attributes of the autonomous systems in end-user decision models. The attributes are characteristics of the system that impact the end-user’s behaviors. Knowing what attributes are important and a general understanding of how the attributes are “weighted” compared to each other is a critical step in end-user decision modelling. The end-user models directly impact the system value model that the designer or engineer uses to assess design decisions. The value model is used by the systems engineer to find the right balance between performance, business concerns, risk, etc. Rigorous identification of model attributes using meaningful human studies is a critical need in systems engineering models of many kinds, including end-user models and system value models. This study identifies attributes and their relative importance from end-users which is immediately applicable to autonomous system MBSE representations.

Hence, engineers may be able to use the study’s information to influence mission engineering analyses which could lead to identifying new autonomous systems that should be developed. Specific mission concepts that are challenging to successfully complete today may indicate that new systems to foster the human-automation interaction are needed. Using the knowledge gained from this article, systems engineers can propose new autonomous systems with specific needed capabilities that user will want to use in mission critical environments and that will improve the effectiveness of human-autonomy teaming and the likelihood of mission success.

6. Limitations and future research

The current study did have its limitations. First, semi-structured interviews were utilized, which limited the sample size because of the large amount of time and resources expended. Second, only students at NPS who were military officers were interviewed, limiting the generalizability of this study. While responses came from SMEs with a wide range of experience, some were enlisted before becoming officers, and some first received their bachelor’s degrees before continuing to become military officers. Further, qualitative analysis can be time consuming as well as require an immense number of resources (student researchers, software, etc.).

Limitations of the current study could be addressed by expanding the sample size in multiple ways such as in military rank (enlisted, rather than exclusively officers), female sample size, and the inclusion of civilians. Multiple participants mentioned that it was important to get the “end user” or lower military personnel’s input because they were the users ultimately using the product. Thus, future studies want to include enlisted military personnel that represent the end-user. Moreover, the inclusion of civilian responses may be used to compare and validate factors to consider for new autonomous system development inside and outside the military context. For instance, future studies could be designed around targeting top ranked factors such as perceived ease of use, reliability, and perceived usefulness, to see if these specific factors are considered important among a more general populous for human-autonomy teaming. Instead of using interviews, a questionnaire could be designed to address these specific factors and could be used to validate the proposed MCTAM model. Moreover, as ordinal data becomes available in the future, systems engineers will be able to use that information to conduct tradeoff studies during system design using swing weighting or multi-attribute utility theory methods.

Acknowledgements

Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the Department of Defense or any other organizations. Approved for Public Release; distribution is unlimited.

Ethical approval

All research activities were approved by the University of Alabama Institutional Review Board (IRB), and approved of compliance with applicable Department of Defense and Department of Navy human research protection policy.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was sponsored by the Department of the Navy, Office of Naval Research, Consortium for Robotics Unmanned Systems Education and Research at the Naval Postgraduate School under Grant [N00244-20-2-0001].

ORCID

Kristin Weger http://orcid.org/0000-0001-7343-8933

Data availability statement

The authors retain copyright of all materials previously published in conference proceedings. Due to the sensitive nature of this research, data are available from the authors after review by Department of Defense/Naval Postgraduate School sponsors.

References

Baker, J. (1975). The DRAGON system—An overview. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, *23*(1), 24–29. https://doi.org/10.1109/TASSP.1975.1162650

Barrett-Pink, C., Alison, L., Maskell, S., & Shortland, N. (2019). On the bridges: Insight into the current and future use of automated systems as seen by Royal Navy personnel. *Journal of Cognitive Engineering and Decision Making*, *13*(3), 127–145. https://doi.org/10.1177/1555343419855850

Bekier, M., Molesworth, B. R., & Williamson, A. (2012). Tipping point: The narrow path between automation acceptance and rejection in air traffic management. *Safety Science*, *50*(2), 259–265. https://doi.org/10.1016/j.ssci.2011.08.059

Benaskeur, A. R., Irandoust, H., Kabanza, F., & Beaudry, E. (2011). *Decision support tool for anti-ship missile defence operations (ADA546901)*. Defence Research and Development Canada Valcartier.

Chavaillaz, A., Wastell, D., & Sauer, J. (2016). System reliability, performance and trust in adaptable automation. *Applied Ergonomics*, *52*, 333–342. https://doi.org/10.1016/j.apergo.2015.07.012

Choi, J. K., & Ji, Y. G. (2015). Investigating the importance of trust on adopting an autonomous vehicle. *International Journal of Human-Computer Interaction*, *31*(10), 692–702. https://doi.org/10.1080/10447318.2015.1070549

Cunningham, M., Regan, M. A. (2015). *Autonomous vehicles: Human factors issues and future research* [Paper presentation]. Proceedings of the 2015 Australasian Road Safety Conference (Vol. 14).

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems. Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Ekman, F., Johansson, M., & Sochor, J. (2018). Creating appropriate trust in automated vehicle systems: A framework for HMI design. *IEEE Transactions on Human-Machine Systems*, *48*(1), 95–101. https://doi.org/10.1109/THMS.2017.2776209

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Endsley, M. R., & Kiris, E. O. (1995). The out-of-the-loop performance problem and level of control in automation. *Human Factors*, *37*(2), 381–394. https://doi.org/10.1518/001872095779064555

Flynn, M., Barr, H., Weger, K., Mesmer, B., Semmens, R., Van Bossuyt, D., & Tenhundfeld, N. (2021). Incentive mechanisms for acceptance and adoption of automated systems. *Systems and Information Engineering Design Symposium (SIEDS)*, 1–6. https://doi.org/10.1109/SIEDS52267.2021.9483740

Ghazizadeh, M., Lee, J. D., & Boyle, L. N. (2012). Extending the technology acceptance model to assess automation. *Cognition, Technology & Work*, *14*(1), 39–49. https://doi.org/10.1007/s10111-011-0194-3

Hall, T. J. (2012). *A case study in design thinking applied through aviation mission support tactical advancements for the next generation (TANG). Department of Information Sciences, vol. Master of Science in Information Technology Management* (p. 185). Naval Postgraduate School.

Hale, B., Van Bossuyt, D. J., Papakonstantinou, N., & O'Halloran, B. (2021). A zero-trust methodology for security of complex systems with machine learning components. In *Proceedings of the ASME 2021 IDETC/CIE*. ASME. https://doi.org/10.1115/DETC2021-70442

Hilburn, B., Westin, C., & Borst, C. (2014). Human vs machine strategies: The impact of strategic conformance on operator workload, performance, and automation acceptance. In *Proceedings of the International Conference on Human-Computer Interaction in Aerospace* (pp. 1–5). ACM. https://doi.org/10.1145/2669592.2669683

Hinchey, M., & Coyle, L. (2010). Evolving critical systems: A research agenda for computer-based systems. In *2010 17th IEEE International Conference and Workshops on Engineering of Computer Based Systems* (pp. 430–435). IEEE. https://doi.org/10.1109/ECBS.2010.56

Hinz, O., Schulze, C., & Takac, C. (2014). New product adoption in social networks: Why direction matters. *Journal of Business Research*, *67*(1), 2836–2844. https://doi.org/10.1016/j.jbusres.2012.07.005

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434. https://doi.org/10.1177/0018720814547570

Hutchins, N., & Hook, L. (2017). Technology acceptance model for safety critical autonomous transportation systems. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)* (pp. 1–5). IEEE. https://doi.org/10.1109/DASC.2017.8102010

Jahanmir, S. F., & Cavadas, J. (2018). Factors affecting late adoption of digital innovations. *Journal of Business Research*, *88*, 337–343. https://doi.org/10.1016/j.jbusres.2018.01.058

Kaber, D. B., Perry, C. M., Segall, N., McClernon, C. K., & Prinzel, L. J. III, (2006). Situation awareness implications of adaptive automation for information processing in an air traffic control-related task. *International Journal of Industrial Ergonomics*, *36*(5), 447–462. https://doi.org/10.1016/j.ergon.2006.01.008

Kaur, K., & Rampersad, G. (2018). Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *Journal of Engineering and Technology Management*, *48*, 87–96. https://doi.org/10.1016/j.jengtecman.2018.04.006

Kyngäs, H., Kääriäinen, M., & Elo, S. (2020). The trustworthiness of content analysis. In *The application of content analysis in nursing science research* (pp. 41–48). Springer. https://doi.org/10.1007/978-3-030-30199-6_5

Landis, J., & Koch, G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159–174.

Levy, Y., & Green, B. D. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a US Navy combat information system. *Journal of Organizational and End User Computing*, *21*(3), 1–23. https://doi.org/10.4018/joeuc.2009070101

Maccuish, D. (2012). Orientation: Key to the OODA loop–the culture factor. *Journal of Defense Resources Management (JoDRM)*, *3*(2), 67–74.

Matsuyama, L., Zimmerman, R., Eaton, C., Weger, K., Mesmer, B., Tenhundfeld, N., Van Bossuyt, D., & Semmens, R. (2021). Determinants that are believed to influence the acceptance and adoption of mission critical autonomous systems. In *AIAA Scitech 2021 Forum* (p. 1156). ARC. https://doi.org/10.2514/6.2021-1156

Militello, L. G., & Klein, G. (2013). Decision-centered design. In J. D. Lee & A. Kirlik (Eds.), *The Oxford handbook of cognitive engineering* (pp. 261–271). Oxford University Press.

Moore, G. A. (2002). *Crossing the chasm: Marketing and selling disruptive products to mainstream customers*. HarperBusiness.

Meyer, J. R. (2020). *Civilian personnel COVID-19 clarification on mission critical functions*. Department of the Air Force.

Papakonstantinou, N., Linnosmaa, J., Alanen, J., Bashir, A. Z., O'Halloran, B., & Van Bossuyt, D. L. (2019). Early hybrid safety and security risk assessment based on interdisciplinary dependency models. In *2019 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1–7). IEEE. https://doi.org/10.1109/RAMS.2019.8768943

Papakonstantinou, N., Linnosmaa, J., Bashir, A. Z., Malm, T., & Van Bossuyt, D. L. (2020). Early combined safety-security defense in depth assessment of complex systems. In *2020 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1–7). IEEE. https://doi.org/10.1109/RAMS48030.2020.9153599

Papakonstantinou, N., Van Bossuyt, D. L., Linnosmaa, J., Hale, B., & O'Halloran, B. (2021). A zero trust hybrid security and safety risk analysis method. *Journal of Computing and Information Science in Engineering*, *21*(5), 050907. https://doi.org/10.1115/1.4050685

Ratchford, M., & Barnhart, M. (2012). Development and validation of the technology adoption propensity (TAP) index. *Journal of Business Research*, *65*(8), 1209–1215. https://doi.org/10.1016/j.jbusres.2011.07.001

Renaud, K., & Van Biljon, J. (2008). Predicting technology acceptance and adoption by the elderly: A qualitative study. In *Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology* (pp. 210–219). ACM. https://doi.org/10.1145/1456659.1456684

Rogers, E. M. (2003). *Diffusion of innovations* (p. 551). Free Press.

Ryan, T. R., Jr., & Mittal, V. (2019). Potential for army integration of autonomous systems by warfighting function. *Military Review*, *99*(5), 122.

Sarter, N. B., Woods, D. D., & Billings, C. E. (1997). Automation surprises. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (2nd ed., pp. 1926–1943). Wiley

Schamber, L. (2000). Time-line interviews and inductive content analysis: Their effectiveness for exploring cognitive behaviors. *Journal of the American Society for Information Science*, *51*(8), 734–744. https://doi.org/10.1002/(SICI)1097-4571(2000)51:8 < 734::AID-ASI60 > 3.0.CO;2-3

Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human–Computer Interaction*, *36*(6), 495–504. https://doi.org/10.1080/10447318.2020.1741118

Strauch, B. (2017). The automation-by-expertise-by-training interaction: Why automation-related accidents continue to occur in sociotechnical systems. *Human Factors*, *59*(2), 204–228. https://doi.org/10.1177/0018720816665459

Taddeo, M., & Blanchard, A. (2021). A comparative analysis of the definitions of autonomous weapons. https://doi.org/10.2139/ssrn.3941214

Taiwo, A., & Downe, A. (2013). The theory of user acceptance and use of technology (UTAUT): A meta analytic review of empirical findings. *Journal of Theoretical and Applied Information Technology*, *49*(1), 48–58.

Van Bossuyt, D. L., Papakonstantinou N., Hale, B., Salonen, J., & O'Halloran, B. (in press). Model based resilience engineering for design and assessment of mission critical systems containing AI components. *Artificial Intelligence and Cybersecurity: Theory and Application*.

About the Authors

Kristin Weger is an Assistant Professor in the Department of Psychology at The University of Alabama in Huntsville. She completed her Ph.D. in 2017 at the University of Bamberg in Industrial Organizational Psychology. Her research has focuses on improving organizational and management processes by focusing on digital transformation and the socio-technical system.

Lisa Matsuyama is a graduate student in the Psychology Department at The University of Alabama in Huntsville. Her research focuses on addressing human factors in system development and the influence of work climate on employee performance.

Rileigh Zimmerman is an undergraduate student at The University of Alabama in Huntsville. She assists in research in the Leadership and Organizational Behavior Lab in the psychology department and her research focuses on factors related to the acceptance and adoption of autonomous systems.

Bryan Mesmer is an Associate Professor in the Department of Industrial and Systems Engineering and Engineering Management at The University of Alabama in Huntsville. He earned his Ph.D. from SUNY at Buffalo. His research reimagines systems engineering using approaches that span traditional areas of decision theory and non-traditional areas.

Douglas Van Bossuyt is a partner at KTM Research, LLC in Tualatin, Oregon. KTM Research specializes in machine vision for manufacturing systems and vision-guided robotics. His research focuses on the intersection of design, system modeling, and risk analysis. He received his PhD from Oregon State University in 2012.

Rob Semmens is an Assistant Professor in the Systems Engineering Department at the Naval Postgraduate School. He earned his Ph.D. from Stanford University, in the Graduate School of Education's Learning Sciences and Technology Design program. His research interests include discovering how people learn about technology while using that technology.

Casey Eaton is a Ph.D. student in the Department of Industrial and Systems Engineering and Engineering Management at the University of Alabama in Huntsville. She completed her M.S. in Systems Engineering (2020) at the University of Alabama in Huntsville. Her research focuses on system modeling and technical measurement.