Human Machine Interface in the Internet of Things (IoT)

Joseph Nuamah  
Department of Industrial and Systems Engineering  
North Carolina A&T State University  
Greensboro, NC USA  
jknuamah@aggies.ncat.edu

Younho Seong  
Department of Industrial & Systems Engineering  
North Carolina A&T State University  
Greensboro, NC 27411  
yseong@ncat.edu

Abstract—Humans would play a central role in IoT systems. The human operator represents one of the most vulnerable in the IoT system, one who can easily be overlooked. In the present study, we sought to accentuate human-in-the-loop issues in System of Systems, and in particular IoT systems through reviewing relevant literature from various perspectives. Some of the issues we highlighted include information visualization, cognition and human trust in intelligent systems. We also explained how neuroergonomics approaches may be employed together with traditional behavioral and subjective measures to improve human-IoT device interactions.

Keywords—Human-in-the-loop; Internet of Things (IoT); Information Visualization; Trust; Neuroergonomics

I. INTRODUCTION

Advancements in information and communication, and sensor technologies have led to generation of tremendous amounts of data. The data generated will be of no value if they cannot be analyzed, interpreted and understood [1]. The Internet of Things (IoT) “allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service” [2]. Keven Ashton [3] was first to use the term “Internet of Things” in the supply chain management domain. Presently, IoT has a broader definition and covers a wide range of domains including utilities, healthcare, transportation, and logistics, etc. [4,5]. Gartner [6] has identified IoT as an emerging technology, and has forecasted it to take 2–5 years for mainstream adoption (see Fig. 1).

IoT application domains may be classified according to network type availability, scale, heterogeneity, user involvement, and impact [7]. For example, Gubbi, Buyya, Marusis, and Palaniswami [8] classified IoT applications into four domains: personal and home, enterprise, utilities, and mobile. Perera, Liu, and Jayawardena [9] reviewed and classified IoT smart solutions based on their application domain into smart wearable, smart home, smart city, smart environment, and smart enterprise. Lee and Lee [10] identified three IoT categories for enterprise applications: monitoring and control, big data and business analytics, and information sharing and collaboration.
for Smart Objects (IPSO), Internet 0, and Web of Things (see Fig. 2). Finally, the “Semantic-oriented” paradigm centers on technologies that organize, represent, and bring meaning to IoT generated information. The overlap between “Internet-oriented” paradigm and “Things-oriented” paradigm highlights the ability of “Things” to connect and exchange information via the Internet. On the other hand, the overlap between “Semantic-oriented” and “Internet-oriented” paradigms, concerns middleware that enable “Things to communicate and understand one another.

Koreshoff, Leong, and Robertson [11] modified Atzori, Iera and Morabito’s framework (see Fig. 2) to a design tool that can be employed by human computer interaction (HCI) practitioners. Their modifications are italicized in Fig. 2 below. In particular, they showed where IoT-related HCI efforts should be focused. For the “Things” paradigm, Koreshoff, Leong, and Robertson [11] indicate that HCI should focus on “‘how computing could be added to everyday objects, and what this can enable”. Regarding the “Internet” paradigm, they suggested that protocols should be selected that enable data to be transmitted to and from objects. The overlap between “Internet” and “Things” paradigms should make HCI researchers cognizant of the physical limitations and communication capabilities of objects when these objects communicate with other objects. The “Semantic” paradigm considers how data could be analyzed and presented in such a way that it makes sense to people. The overlap between the “Internet” and “Semantic” highlights the fact HCI designers need to design objects that fit with other objects and that they should consider how they are designing will interface with existing objects. Lastly, relevant to the present study is the overlap between the “Things” and “Semantic” paradigms. This overlap accentuates how data could be presented by IoT devices in ways that make sense to people.

The aim of this paper is to accentuate human-in-the-loop issues in System of Systems, and in particular IoT systems through review of relevant literature in various perspective. We seek to highlight the need for engineers and system designers to view the human operator as a central figure in the design and operation of IoT systems. The human operator is the key to success in IoT applications. The rest of this paper is organized as follows. First, we present sensor networks and data fusion as key enablers in IoT systems. Next, we explain the importance of information visualization to the human operator, and human trust in automation. This is followed by sections on cognition and neuroergonomics.

II. SENSOR NETWORKS AND DATA FUSION

Sensors networks are a major enabler of IoT. “Data fusion techniques combine data from multiple sensors and related information from associated databases to achieve improved accuracy and more specific inferences than could be achieved by the use of a single sensor alone”[12]. The Joint Directors of Laboratories (JDL) data fusion model, used to widely used for categorize data fusion functions, has five data fusion levels: Level 0 (signal/feature assessment), level 1 (entity assessment), level 2 (situation assessment), level 3 (impact assessment), level 4 (process assessment), and Level 5 [13]. Level 5 fusion level was added to the data fusion model to underscore the need to focus and improve on the human system interaction [13, 14].

Hall, Hall, and McMullen [13] illustrate (see Fig. 3) the data fusion process as an energy-driven process in which sensors passively or actively collect energy. This energy is then transformed into state vectors, labels, and knowledge.

Much of the research in data fusion has focused on automatic tracking and target recognition. Even though this kind of research is needful, current problems are much more complex than that. This is because the data required to tackle current problems include sensor data, textual data, and utilization of models [13]. Analysis of these problems is labor intensive, and requires analysts to explore data, and interpret results. Hall, Hall, and McMullen [13] express the need to improve human interaction with data fusion systems, and advocate innovate HCI designs.

Fig. 2. Modified “Internet of Things” paradigms. Source: Koreshoff, Leong, & Robertson [11].

Fig. 3. Transformation of energy into knowledge. Source: Hall, Hall, and McMullen [13].

III. INFORMATION VISUALIZATION

Data collected by sensors would have to be transformed into meaningful and task relevant information. This information must be presented in a format that human operators can cope with. Robertson, Czerwinski, Fisher, and Lee [15] define information visualization as “the art and science of representing abstract information in a visual form that enables human users to gain insight through their perceptual and cognitive capabilities” [15]. The tremendous amount of data generated by sensor networks would make operators susceptible to information overload, which could have negative effects on performance [16]. Visualization allows the operator of an IoT application to interact with the environment [8]. Depending on how information is presented, humans are able to extract patterns from large amounts of data with relative ease. Computers are designed to process massive volumes of data within a relatively short time. However compared to humans, computers find it difficult detecting patterns. Traditional decision aids and visualization tools are designed in such a way that they either accentuate the strengths of computers or their human operators, but not both. Humans are able to speedily make sense of partial, incomplete or rapidly presented information, but are unable to cognitively process large amounts of rapidly changing information. Computers, on the other hand, have rapid data processing capabilities. Consequently, it is needful to combine the fast data processing capabilities of computers with intuitive decision making skills of humans [17] to improve human information throughput and decision making. IoT applications would need to present information in an intuitive and easy to understand format [10].

In operational environments where operators do not have direct access to the environment, they access data about the state of the environment through a technological interface. System designers should be able to control how information is presented to operators [16]. The design of these interfaces requires an understanding of the judgment attributes that they are to support and the effect of their design on operator judgment [18]. It is important that these interfaces present information in a way that allows the operator to understand the current situation. For instance, graphical representations induce intuitive cognition [19], take advantage of human pattern-matching abilities, and enable speedy detection of out-of-parameter system states [20]. The cognitive fit between task type and the format in which information is presented leads to optimal decision making [21, 22]. Furthermore, Hammond, Hamm, Grassia and Pearson [23] found that higher correspondence between task characteristics and cognitive characteristics was correlates in a significant way with an operator’s judgment accuracy. Thus, understanding judgment and decision making performance centered on the format of information display and the cognitive strategy adopted by the decision maker may help designers of human-machine systems design more effective screen displays, thereby improving judgment performance.

IV. HUMAN TRUST IN AUTONOMOUS SYSTEMS

Management of trust is essential to reducing uncertainty and building user acceptance of IoT devices and services [24]. Roman, Zhou, and Lopez [25] considered two dimensions of trust in IoT: trust in the interactions between entities, and trust in the IoT system from the users’ perspective. The present study is interested in the latter dimension. Yan, Zhang, and Vasilakos [26] described the IoT system as consisting of three layers: a physical perception layer, a network layer, and an application layer. They presented 10 trust management objectives of which the ninth, Human-Computer Trust Interaction (HCTI), is of relevance to the present study. Yan, Zhang, and Vasilakos [26] suggest the need to provide IoT users with sound usability and trustworthy human-computer interaction. They acknowledged the fact that HCTI has been ignored in previous studies, but were quick to add that it is one of the "decisive aspects that will impact the final success of IoT".

Madsen and Gregor [27] defined human-computer trust as “the extent to which a user is confident in, and is willing to act on the basis of, the recommendations, actions, and decisions of an artificially intelligent decision aid”. This definition entails the decision maker’s confidence in the decision aid and his or her willingness to act based on the decision aid’s decisions and advice. Although trust is not the only factor that influences the operator’s reliance on an automated system, it certainly is one of several attitudes an operator holds which combine to form his or her intention to use automated capabilities. It is a critical requirement for the success of any automated solution [28, 29].

After reviewing earlier models and definitions of trust, Lee and See [30] defined trust in automated systems as “an attitude that an agent will help achieve an individual’s goals in a situation characterized by uncertainty and vulnerability”. This trust is an attitude based on the human operator’s beliefs and perceptions with respect to different system characteristics. The perceived state of system attributes influences the human operator’s trust in automation. They presented three different cognitive processes that use these perceptions to form attitudes of trust; (1) analytic process, (2) analogical process, and (3) affective process. The interplay of these processes depends on the evolution of the relationship between the operator and automation, the information available to the operator, and the way the information is displayed. The analytic process is a cognitively demanding process in which the information presented is deliberately processed based on the human operator’s knowledge, experience, and mental model of the system. The analogical process requires less cognitive resources and trust is based on the perceived automation system’s characteristics, and other factors such as reputation or third-party information. The affective process influences trust on the basis of emotions. The operator does not only trust the system based on what they think about it but also on what they feel about it. In an instance where rules fail to apply and cognitive resources are unavailable, an operator’s behavior may be guided by emotions. People are more likely to employ analytical processing than analogic processing when adequate cognitive resources are available. On the other hand, people are more likely to employ analogic and affective processing when
insufficient cognitive resources are available. Trust is affected by the content and format of the display. When information is displayed in a consistent and clearly organized manner, trust tends to increase. They suggested that an appropriate trust in automation may be engendered if information about the automation is presented in a way compatible with the analytic, analogical and affective processes.

Hoff and Bashir [31] reviewed empirical research on factors that influence trust in automation and presented three interdependent layers of variability in human-automation trust. These are dispositional trust, situational trust, and learned trust. Dispositional trust relates to an individual’s overall tendency to trust automation. Factors that influence dispositional trust are culture, age, gender and personality traits. Situational trust depends on the external environment and the internal, context-dependent characteristics of the individual. Learned trust relates to an individual’s evaluations of a system based on past experience or the present interaction. They suggest that trust in an automated system can be promoted by increasing the system’s transparency, politeness, and ease of use.

Relevant system attributes have been empirically found to influence human trust in automation. Jenkins, Wollocko, Farry, and Voshell [32] present a summary of system and operator attributes known to influence trust. They described Sheridan [33]’s seven attributes humans use to assign trust: understandability, predictability, familiarity, explanation of intention, usability, competence, and reliability, and added that operator attributes include faith, background knowledge, personal attachment, personality, extraversion, and propensity to trust machines. Trust progresses from predictability, through dependability to faith with time [34]. The human operator first evaluates the predictability of a system by assessing the consistency and desirability of its repeated behavior. With time, as the system consistently convert input into output, dependability becomes a basis of trust. Faith develops after a period of time. According to Jenkins, Wollocko, Farry, and Voshell [34], information obtained from third parties, general assumptions and stereotypes may affect the faith that operators have in automation. Apart from this exception, operators must first decide to rely on the automated system before a (positive or negative) change in their trust can take place. A change in an operator’s trust can occur when there is a difference between the automation’s perceived current capabilities and the automation’s perceived capabilities during prior recent states of reliance [34].

Seong and Bisantz [35] investigated calibrating human trust in automated decision aids. One of their hypotheses was that trust assessments would be better calibrated with the presence of meta-information. Meta-information about the decision aid was provided to participants using a Lens Model based feedback. They found that operators who were given the meta-information performed significantly better than those who were not given the meta-information. However, the study did not examine the effect of different types of interface display on human trust in automated decision aids.

V. COGNITION AND TASK CORRESPONDENCE

Previous researchers have used dual process theories to explicate the human cognitive system. The theories are supported by much evidence in cognitive science [36], have been the focus of contemporary research [37, 38, 39, 40] and have had various labels attached to each of one of them. Theorists assume that cognitive tasks evoke two types of decision making processes—analytical and intuition. Analytical cognition is conscious, effortful, and requires cognitive resources. Intuitive cognition is automatic, nonverbal, associative, rapid, effortless, concrete, holistic, and requires minimal cognitive resources. In human-automation interactions, information presented to the operator may be in a format that elicits intuition or analytical cognition.

Patterson [41] found that taxonomies used to classify human automation interactions consider only analytical cognition and neglect intuition cognition. He modified the human automation taxonomy proposed by Parasuraman, Sheridan, and Wickens [42] by adding six new automation levels (see Fig. 4). He claimed that earlier taxonomies ignored intuition cognition, but which he said is the better of the two modes of cognition whenever automation fosters a “quick grasp of the meaningful gist of information based on experience or perceptual cues, without working memory or precise analysis”. Analysis cognition, on the other hand, is better “whenever automation requires reading, remembering information via working memory, rule-based reasoning, hypothetical thinking, deliberation, or precise analysis”. He stated that future automated systems may be improved if they incorporate both analytical and intuitive cognition.

VI. NEUROERGONOMICS

Human factors engineering seeks to study human capabilities and limitations that affect the design of human-automation interactions [43]. As human factors practitioners, we are interested in the human-in-the-loop evaluation of automated, autonomous and/or IoT systems. This kind of evaluation includes a human, whether in an active or passive capacity in the participant role [44]. Traditional behavioral and subjective methods employed by system designers to evaluate human-automation interactions may be inadequate [45]. Psychophysiology allows for the use of physiological measurements to understand an operator’s behavior by non-invasively recording peripheral and central physiological changes while the operator behaves under controlled conditions.
Neuroergonomics, defined as the study of brain and behavior [46] allows human-automation researchers to study and develop new frameworks about humans and work than an approach based solely on the measurement of subjective perceptions or overt performance of the HO [47]. It asserts that the human brain must be examined during interaction with the environment to enable a complete understanding of cognition, action, and environment.

Some issues that arise in the context of human-automation interaction and by extension human-IoT interaction include (1) how the operator can be kept continuously aware of the state of the system to prevent an out-of-the-loop unfamiliarity, (2) how multimodal information should be presented to the operator, and (3) how information can be presented in a format that is consistent with the operator’s mental representation of the system. This is where neuroergonomics will be most effective. Neuroergonomics approaches may be used to evaluate, among other things, the usability of IoT devices. Psychophysiological measures can be used to determine whether a particular display or control device produces a general difference in brain function. The psychophysiological information, along with behavioral and subjective assessments, can then be used to determine whether the modified system produces same human responses as compared to a baseline system [43].

The ability to unobtrusively and continuously monitor operator mental states in a given task in an operational environment could be beneficial in finding more efficient and effective methods for humans to interact with IoT devices [45]. Task engagement, attention, and workload are examples of mental states that may be monitored. The information obtained could be exploited in an offline analysis for improving smart wearable devices, smart home devices, user interface of cars and many other IoT applications [48]. Neuroergonomics may be applied in a variety of domains. These include aviation, driving, brain-computer interfaces, and virtual reality [46].

VII. CONCLUSION

Humans would play a central role in IoT systems. The human operator represents one of the most vulnerable in the IoT system, one that can easily be overlooked. This paper sought to accentuate human-in-the-loop issues in system of systems, and in particular IoT systems. Some of the issues include information visualization, cognition and trust. We also explained how neuroergonomics approach may be employed together with traditional behavioral and subjective measures to improve human-IoT device interactions.

ACKNOWLEDGMENT

This material is partially based on research sponsored by Air Force Research Laboratory and OSD under agreement number FA8750-15-2-0116, and partially by US Army RDECOM (W911NF-13-1-0118). The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory and OSD or the U.S. Government.

REFERENCES


