Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust

Kevin Anthony Hoff and **Masooda Bashir**, University of Illinois at Urbana-Champaign

Objective: We systematically review recent empirical research on factors that influence trust in automation to present a three-layered trust model that synthesizes existing knowledge.

Background: Much of the existing research on factors that guide human-automation interaction is centered around trust, a variable that often determines the willingness of human operators to rely on automation. Studies have utilized a variety of different automated systems in diverse experimental paradigms to identify factors that impact operators' trust.

Method: We performed a systematic review of empirical research on trust in automation from January 2002 to June 2013. Papers were deemed eligible only if they reported the results of a human-subjects experiment in which humans interacted with an automated system in order to achieve a goal. Additionally, a relationship between trust (or a trust-related behavior) and another variable had to be measured. All together, 101 total papers, containing 127 eligible studies, were included in the review.

Results: Our analysis revealed three layers of variability in human–automation trust (dispositional trust, situational trust, and learned trust), which we organize into a model. We propose design recommendations for creating trustworthy automation and identify environmental conditions that can affect the strength of the relationship between trust and reliance. Future research directions are also discussed for each layer of trust.

Conclusion: Our three-layered trust model provides a new lens for conceptualizing the variability of trust in automation. Its structure can be applied to help guide future research and develop training interventions and design procedures that encourage appropriate trust.

Keywords: trust in automation, human–automation interaction, automated system, trust formation, reliance

Address correspondence to Masooda Bashir, University of Illinois at Urbana-Champaign, 1308 West Main St., Urbana, IL 61801-2307, USA; e-mail: mnb@illinois.edu.

HUMAN FACTORS
Vol. 57, No. 3, May 2015, pp. 407–434
DOI: 10.1177/0018720814547570

INTRODUCTION

At its most basic level, trust is an adhesive that connects people from all over the globe. It measures the degree of confidence individuals have in strangers or the degree to which romantic partners believe in the fidelity of their significant other. Communities, organizations, governments, nations, cultures, and societies can all be explained, in part, by trust. Yet the significance of trust is not limited to the interpersonal domain; trust can also define the way people interact with technology. In particular, the concept of *trust in automation* has been the focus of substantial research over the past several decades. Automated technologies are everywhere in the modern world, from flight management systems to GPS route planners. Automation can be used to acquire and analyze information, make decisions, carry out actions, or monitor other systems (Parasuraman, Sheridan, & Wickens, 2000). When human–automation teams perform optimally, the efficiency of labor systems can improve drastically. Unfortunately, optimum performance is not always achieved, as using automation can complicate otherwise simple tasks. Additionally, the introduction of automation into critical systems, such as hospitals, aircraft, and nuclear power plants, has created new pathways for error, sometimes with grave consequences.

Just as it does in interpersonal relationships, trust plays a leading role in determining the willingness of humans to rely on automated systems in situations characterized by uncertainty. Accidents can occur when operators misuse automation by overtrusting it, or disuse automation as a result of undertrusting it (Parasuraman & Riley, 1997). Facilitating appropriate trust in automation is key to improving the safety and productivity of human–automation teams.

In order to better understand the factors that influence operators' trust, researchers have stud-

ied the trust formation process using a variety of automated systems in diverse experimental paradigms. Lee and See (2004) provide an integrated review of early research in this area to elucidate the role of trust, and the feelings associated with it, in guiding human behavior toward automation. Their thought-provoking paper triggered numerous studies on specific factors related to trust in automation that have greatly expanded knowledge regarding the variability of trust. However, because of the wide diversity of variables studied using distinct methodologies, a cohesive analysis is needed to synthesize recent findings. In this paper, we build on the work of Lee and See by presenting the results of a systematic review of recent empirical research (published between January 2002 and June 2013) on factors that influence human–automation trust and reliance. Our extensive analysis culminates in a three-layered trust model that can be applied to a variety of situations with unique automated systems and diverse human operators. The model provides a new lens for conceptualizing the variability of trust in automation. Design recommendations and future research directions are also presented and discussed.

AUTOMATION

Automation can be defined as "technology that actively selects data, transforms information, makes decisions, or controls processes" (Lee & See, 2004, p. 50). One of the primary values of automation is its ability to perform complex, repetitive tasks quickly without error. Human–automation labor systems can be extremely efficient, because the use of automation gives people more freedom to focus their attention where it is needed. Today, automated systems perform countless tasks for which humans once had responsibility. Another advantage of automation is that it can be used in place of people in hazardous environments. A well-known example of such automation is the Predator Drone, which has been used by the U.S. military in conflicts in Afghanistan, Iraq, and numerous other combat zones.

There are four primary types of automated systems, including information acquisition, information analysis, decision selection, and action implementation (Parasuraman et al., 2000). An additional type of automation is automation whose sole purpose is to monitor other automated systems. These categories are not mutually exclusive; a single automated system can fall into more than one category if it performs multiple functions.

In addition to type, automated systems vary based on the amount of control the human operator has over their functions. Parasuraman et al. (2000) outline a 10-level scale that classifies automation based on its locus of control. At Levels 1 through 5, the human has overall control of a task but uses automation in incrementally increasing amounts for assistance. At Levels 6 through 10, automation performs tasks independently, providing operators with less feedback at each level up the scale (Parasuraman et al., 2000).

Automation-related accidents can occur for a variety of reasons, including, but not limited to, poor system design, organizational factors, software and hardware failures, environmental interference, operator abuse, operator misuse, and operator disuse (Parasuraman & Riley, 1997). Trust is particularly relevant to misuse and disuse of automation, as trust plays a critical role in guiding human–automation reliance. For example, the *Costa Concordia* cruise ship disaster that killed 32 passengers in January 2012 may have been the result of the captain's undertrusting of the ship's navigation system in favor of manual control. Ensuing investigations discovered that the captain diverged from the ship's computer-programmed route before hitting the shallow reef that caused the sinking (Levs, 2012). Overtrust in automation may have contributed to the crash of Turkish Airlines Flight 1951 in February of 2009. The crash, which killed nine people, including all three pilots, was partially caused by the pilots' continued reliance on the plane's automatic pilot after an altitude-measuring instrument failed ("Faulty Reading Helped," 2009). Those are but two of many accidents that have been linked to misuse and disuse of automation.

Instilling operators with appropriate levels of trust in automation can reduce the frequency of misuse and disuse (Lee & See, 2004). Doing so effectively, however, can be far more difficult

than might seem. Inconsistent characteristics of the operator, environment, and automated system can alter the trust formation process in unforeseen ways. In order to conceptualize that variability, some researchers have attempted to model the trust formation process by drawing on trust research from other fields (e.g., interpersonal trust in Madhavan & Wiegmann, 2007b). The following section summarizes the literature on trust, with an emphasis on trust in other people.

TRUST

The concept of trust can be found in various fields of research. Investigators from psychology, sociology, philosophy, political science, economics, and human factors have tried to make sense of trust and develop ways to conceptualize the term. Mayer, Davis, and Schoorman (1995) authored one of the most influential review papers on trust to date by thoroughly examining literature on the antecedents and outcomes of organizational trust. In the human factors domain, considerable research has focused on the role of trust in guiding interactions with different technologies. For example, Corritore, Kracher, and Wiedenbeck (2003) developed a model of online trust that conceptualizes trust variability based on perceptions of website risk, credibility, and ease of use. Gefen, Karahanna, and Straub (2003) explore the role of trust and the technology acceptance model in online shopping environments. Hoffmann et al. (2009) discuss the role of trust, as well as antitrust, in creating and minimizing security risks in cyberdomains.

An important commonality across the various fields of research is that almost every explanation of trust includes three components. First, there must be a truster to give trust, there must be a trustee to accept trust, and something must be at stake. Second, the trustee must have some sort of incentive to perform the task. The incentive can vary widely, from a monetary reward to a benevolent desire to help others. In interactions with technology, the incentive is usually based on the designer's intended use for a system. Finally, there must be a possibility that the trustee will fail to perform the task, inviting uncertainty and risk (Hardin, 2006). These elements outline the idea that trust is needed when something is exchanged in a cooperative relationship characterized by uncertainty. This applies to both interpersonal and human–automation relationships. Still, although the significance of trust in cooperative relationships is generally agreed upon, inconsistencies remain regarding the exact definition of trust.

Defining Trust

Authors of the earliest investigations of trust attempted to define it in a general sense, without any sort of context. Rotter (1967) began by describing trust as a disposition toward the world and the people in it. This definition has since grown to be more content and situation specific. Barber (1983) viewed interpersonal trust as a set of socially learned expectations that vary based on social order, whereas Pruitt and Rubin (1986) see trust as a number of beliefs about others. Whereas those authors view trust as a belief or attitude, other authors have defined it as a willingness to accept vulnerability (Mayer et al., 1995) and a behavioral state of vulnerability (Deutsch, 1960). Clearly, scholars are far from reaching a consensus on a single definition of trust. Nevertheless, because it is possible to trust someone without recruiting his or her assistance, we think trust should be viewed as a mental state. For this paper, we will rely on Lee and See's (2004) definition of trust as "the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability" (p. 54).

Trust is always grounded on at least one quality or characteristic of a trustee. In a thorough review of trust literature, Mayer et al. (1995) established three general bases of trust: ability, integrity, and benevolence. The stability of one's trust varies depending on which of the aforementioned qualities it refers to. For example, if trust is based on the ability of a trustee, it will vary depending on how well the trustee performs a task. Trust grounded on the integrity of a trustee depends not on the actual performance of a trustee but on the extent to which the trustee's actions match the values of the truster. Finally, the stability of benevolence-based trust is contingent upon whether the trustee's actions match the goals and motivations of the truster (Lee & See, 2004). When trust is based primarily on the integrity or benevolence of a trustee,

poor performance alone will not significantly damage it.

Trust formation is quite often a dynamic process. As people are exposed to new information, feelings of trust can change drastically. This change can happen at both the conscious and unconscious levels. The following section describes the various processes by which trust is formed, maintained, and destroyed.

Trust Formation

The formation of trust involves both thinking and feeling, but emotions are the primary determinant of trusting behavior (Lee & See, 2004). For example, individuals often decide not to trust others simply because of uneasy feelings that cannot be explained rationally. *Affective processing* cannot be overlooked when attempting to understand trust formation and any resulting behavior. Without emotions, trust would not have such a profound impact on human behavior (Lee & See, 2004).

Although feelings likely have the greatest influence on trusting behavior, both feelings and behavior depend on thoughts. These thoughts may take the form of analogic or analytic judgments. *Analogic* thought processes utilize societal norms and the opinions of others to determine trustworthiness. The *analytic* process of trust formation, on the other hand, involves rational evaluations of a trustee's salient characteristics (Lee & See, 2004). When sufficient cognitive resources are available, people may be more likely to use analytic processing. When cognitive resources are limited, however, people are more likely to rely on analogic and affective thought processes, both of which can occur rapidly outside of conscious awareness.

Although many people fail to recognize it, we as humans automatically make judgments about the trustworthiness of people we meet on a day-to-day basis. These snap judgments are not always accurate, but humans have a remarkable talent for accurately assessing the trustworthiness of others using subtle cues. Engell, Haxby, and Todorov (2007) used functional magnetic resonance imaging (fMRI) to show that the amygdala (a portion of the brain located in the medial temporal lobe) is utilized during rapid evaluations of the trustworthiness of human faces. In their experiment, subjects' amygdala responses increased as they were exposed to faces that were previously rated as less trustworthy (Engell et al., 2007). This finding is consistent with that of Willis and Todorov (2006), who found that 100 ms of exposure to a novel face is enough time to make initial judgments of the face's trustworthiness. These two studies point to a dissociation between the automatic engagement of the amygdala and the intentional engagements of other neural mechanisms during interpersonal trust formation. Still, although humans are capable of making instinctive assessments of the trustworthiness of other people, this ability does not directly translate to technological systems. The next section explains the nature of human–automation trust.

HUMAN–AUTOMATION TRUST

Although trust in technology is different from interpersonal trust, parallels exist between the two. At the most fundamental level, the two types of trust are similar in that they represent situation-specific attitudes that are relevant only when something is exchanged in a cooperative relationship characterized by uncertainty. Beyond this conceptual likeness, research has found more specific similarities. For example, several studies in the 1990s showed that people apply socially learned rules, such as politeness, to interactions with machines (Nass, Moon, & Carney, 1999; Nass, Steuer, & Tauber, 1994). Furthermore, neurological research suggests that some of the same neural mechanisms utilized by participants in interpersonal trust games are also used in trust-based evaluations of eBay website offers (Dimoka, 2010; Riedl, Hubert, & Kenning, 2010). One potential reason for these similarities is that to some degree, people's trust in technological systems represents their trust in the designers of such systems (Parasuraman & Riley, 1997). In this way, human–automation trust can be viewed as a specific type of interpersonal trust in which the trustee is one step removed from the truster. Regardless of how human–automation trust is conceptualized, important differences exist between it and interpersonal trust in regard to what it is based on and how it forms (Madhavan & Wiegmann, 2007b).

Distinctions Between Human–Automation and Interpersonal Trust

Human–automation trust and interpersonal trust depend on different attributes. Whereas interpersonal trust can be based on the ability, integrity, or benevolence of a trustee (Mayer et al., 1995), human–automation trust depends on the performance, process, or purpose of an automated system (Lee & Moray, 1992). Performance-based trust, similar to Mayer et al.'s (1995) ability-based trust, varies depending on how well an automated system executes a task. Process-based trust, analogous to integrity-based trust in humans, fluctuates based on the operator's understanding of the methods an automated system uses to perform tasks. Last, purpose-based trust is contingent upon the designer's intended use for an automated system.

The progression of interpersonal trust formation also differs from that of human–automation trust (Madhavan & Wiegmann, 2007b). Rempel, Holmes, and Zanna (1985) explain that interpersonal trust is initially based on the mere predictability of a trustee's actions because people tend to enter relationships with strangers cautiously. As interpersonal relationships progress, the dependability or integrity of a trustee becomes the core basis of trust. Finally, fully mature interpersonal relationships are based on faith or benevolence (Lee & See, 2004). On the other hand, human–automation trust often progresses in the reverse order. Evidence suggests that people often exhibit a positivity bias in their trust of novel automated systems (Dzindolet, Peterson, Pomranky, Pierce, & Beck, 2003). People commonly assume that machines are perfect. Therefore, their initial trust is based on faith. However, this trust rapidly dissolves following system errors; as relationships with automated systems progress, dependability and predictability replace faith as the primary basis of trust (Madhavan & Wiegmann, 2007b).

It is important to note that the trend just described is applicable only to relationships with unfamiliar trustees and automated systems. In the real world, the trust formation process depends on a number of factors related to the operator, environment, and automated system. We sought out to conceptualize that variability by systematically reviewing recent empirical research on trust in automation.

Literature Review Methodology

A literature review of empirical research on trust in automation (published anytime between January 1, 2002, and June 31, 2013) was conducted in order to build on the previous review conducted by Lee and See (2004). Using combinations of key terms, such as *trust, reliance, automation, automated system*, and *decision support system*, an initial search of eight library databases (PsycINFO, PsycARTICLES, PsycBOOKS, Engineering Village, IEEE Xplore, Conference Index, ProQuest Dissertations and Theses, and Scopus) yielded 1,981 records consisting of conference papers, journal articles, technical reports, dissertations, and theses. All 1,981 records were screened for eligibility based on the following criteria:

1. The paper had to report the results of a novel human-subjects experiment.
2. In the experiment, participants had to interact with an automated system while working to achieve a goal.
3. A relationship between trust (or a trust-related behavior) and another variable had to be measured.

The initial search procedures led to the identification of 89 potentially eligible papers, which were carefully evaluated based on their relevance to the topic, reported methodology, originality of findings, and source publication. That process led to the disqualification of 12 papers (most of which were judged to be unoriginal in that they reported the results of an experiment already discussed in a different paper), leaving a total of 77 eligible papers.

Keywords found in the 77 eligible papers were then used in a secondary web search (using Google and Google Scholar). Reference lists were also scanned to locate papers not found in the web searches. These secondary processes resulted in the identification of 24 additional papers. Altogether, 101 papers, consisting of 127 unique studies (as several of the papers report the results of multiple experiments), were included in the qualitative review. As the studies

TABLE 1: Types of Automated Systems Used in Eligible Studies

Type of System	Number of Studies (*N* = 127)	Percentage of Total
Combat identification aid	31	24.4
General decision aid	25	19.7
Fault management/task monitoring aid	24	18.9
Automated weapons detector (luggage)	11	8.7
Target identification aid (noncombat)	9	7.1
Collision warning system	9	7.1
Route-planning system	7	5.5
Other	11	8.7

TABLE 2: Categories of Automation Used in Eligible Studies

Category of Automation	Number of Studies (*N* = 127)	Percentage of Total
Decision selection	95	74.8
Information analysis	25	19.7
Action implementation	5	3.9
Information acquisition	2	1.6

were analyzed, several additional papers that did not meet eligibility requirements were added in order to fill empirical research gaps. The additional papers, which are noted when introduced, all involved trust in some way but were not directly related to automation. Instead, they focused on trust in e-commerce websites, social robots, or on-screen computer agents.

Empirical Research Overview

The 127 eligible studies employed a variety of different automated systems in diverse experimental paradigms. As can be seen in Table 1, the most commonly studied systems were combat identification aids, followed by general decision aids and fault management/identification aids. Table 2 summarizes the most commonly studied categories of automation (Parasuraman et al., 2000). As can be seen, the vast majority of studies (~75%) utilized decision selection automation. This trend likely reflects the fact that decision selection automation is typically more complex and thus requires a high level of trust from operators.

Considerable variability also exists in how the eligible studies measured trust in automation. Of the 127 studies included in the analysis, 34% (n = 43) measured trust by assessing trusting behaviors (e.g., reliance on or compliance with automation), 4% (n = 5) used self-report questionnaires, and 62% (n = 79) used both trusting behaviors and self-report measures. One of the most commonly used self-report scales was developed by Jian, Bisantz, Drury, and Llinas (2000). Their questionnaire was designed to represent 12 factors of trust between humans and automation that were determined through a three-phased experiment. Other researchers who used self-report measures designed their own trust scales (e.g., Merritt & Ilgen, 2008; Merritt, 2011) or measured related concepts, such as system confidence (e.g., Lerch, Prietula, & Kulik, 1997).

In order to integrate the findings of the wide-ranging studies in this area, we consider trust in a general sense. Our analysis builds toward a model of factors that influence trust in automated systems. The model's basic three-layered structure (see Figure 1) can be applied to a variety of situations with different automated systems and human operators. In the next section, we examine the sources of variability in the formation and maintenance of trust in automation.

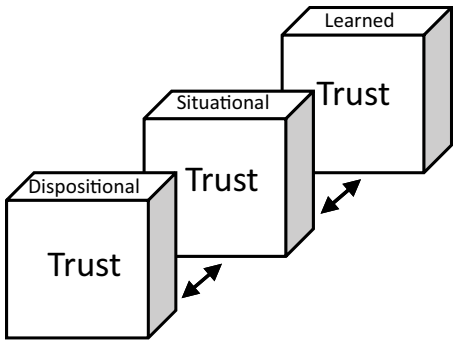

Figure 1. Three-layered framework for conceptualizing trust variability.

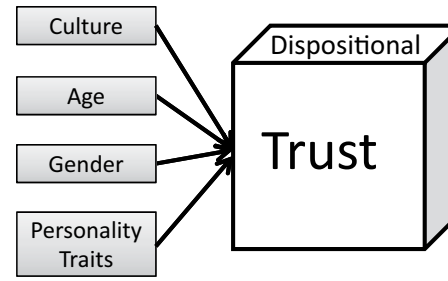

Figure 2. Factors that influence dispositional trust.

EMPIRICAL RESEARCH ON FACTORS THAT INFLUENCE TRUST

Our analysis revealed three broad sources of variability in human–automation trust: the human operator, the environment, and the automated system. These variables respectively reflect the three different layers of trust identified by Marsh and Dibben (2003): dispositional trust, situational trust, and learned trust. Dispositional trust represents an individual's enduring tendency to trust automation. Situational trust, on the other hand, depends on the specific context of an interaction. The environment exerts a strong influence on situational trust, but context-dependent variations in an operator's mental state can also alter situational trust. The final layer, learned trust, is based on past experiences relevant to a specific automated system. Learned trust is closely related to situational trust in that it is guided by past experience (Marsh & Dibben, 2003); the distinction between the two depends on whether the trust-guiding past experience is relevant to the automated system (learned trust) or to the environment (situational trust). Although the three layers of trust are interdependent, they will be examined separately in this section, beginning with dispositional trust.

Dispositional Trust

Just as in the interpersonal domain, individuals exhibit a wide variability in their tendency to trust automation. Unlike context-dependent characteristics, such as mood and self-confidence, dispositional variations can alter trust formation in every situation. *Dispositional trust* represents an individual's overall tendency to trust automation, independent of context or a specific system. Whereas research on the biology of trust has shown that genetics play an important role in determining interpersonal trust propensity (Riedl & Javor, 2012), we use the term *dispositional trust* to refer to long-term tendencies arising from both biological and environmental influences. Thus, the defining characteristic of dispositional trust is that it is a relatively stable trait over time, unlike situational and learned trust. Our review revealed four primary sources of variability in this most basic layer of trust: culture, age, gender, and personality (see Figure 2).

Culture. Culture is a particularly important variable, because it is something that nearly everyone identifies with. In the interpersonal domain, substantial research has shown that trust varies across countries, races, religions, and generational cohorts (e.g., Naef, Fehr, Fischbacher, Schupp, & Wagner, 2008). To date, however, very few studies have focused on the role of culture in trust in automation. In one recent study, Huerta, Glandon, and Petrides (2012) found that Mexicans are more likely to trust automated decision aids and less likely to trust manual decision aids, compared to Americans. Several studies have also found cultural differences in how people perceive social robots (Li, Rau, & Li, 2010; Rau, Li, & Li, 2009). Although these studies suggest that culture-based variables can be relevant to trust in automation, more research is needed.

Age. Age differences in trust in automation may be the result of cognitive changes, cohort effects, or some combination of both variables

(Czaja & Sharit, 1998; Ho, Kiff, Plocher, & Haigh, 2005). Several studies have shown age to be a significant variable. Ho, Wheatley, and Scialfa (2005) showed that older adults trust and rely on decision aids more than younger adults, but they do not calibrate their trust any differently following automation errors. In contrast, Sanchez, Fisk, and Rogers (2004) found that older adults were better at calibrating their trust to the changing reliability of a decision support system. A recent study by Pak, Fink, Price, Bass, and Sturre (2012) showed that adding a picture of a physician to the interface of a diabetes management application led younger participants to place greater trust in the system's advice but had no effect on older participants' trust. Overall, this research and other findings (e.g., Ezer, Fisk, & Rogers, 2007, 2008; McBride, Rogers, & Fisk, 2010, 2011; McCarley, Wiegmann, Wickens, & Kramer, 2003) suggest that people of different ages may employ different strategies when analyzing the trustworthiness of automated systems. However, the specific effect of age likely varies in distinct contexts. (For a review of age-related research, see Steinke, Fritsch, & Silbermann, 2012.)

Gender. Consistent gender differences have not yet surfaced in studies focused solely on trust in automation. However, research has shown that gender can play a role in guiding interactions with other types of technology. For example, E. J. Lee (2008) found that women are susceptible to flattery from computers, whereas men display negative reactions to it. This discrepancy, and gender-based research on human–robot interaction (e.g., Nomura, Kanda, Suzuki, & Kato, 2008; Tung, 2011), suggests that males and females may respond differently to an automated system's communication style and appearance. Thus, even though consistent differences have not been found, the prospective gender of an automated system's operator should be factored into the design process of certain systems.

Personality. An operator's personality traits are the final component of dispositional trust. In the interpersonal domain, dispositional trust is, itself, an enduring personality trait that represents an individual's tendency to trust other people throughout life. There are numerous psychometric scales that measure this tendency (e.g., Rempel et al., 1985; Rotter, 1980), and research has shown that it is a significant determinant of human behavior (Colquitt, Scott, & LePine, 2007).

Several researchers have attempted to apply the dispositional trust construct to human–automation interaction in an attempt to differentiate people based on their propensity to trust automated systems. Biros, Fields, and Gunsch (2003) showed that participants with greater dispositional trust in computers displayed more trust in information from an unmanned combat aerial vehicle. In a later study, Merritt and Ilgen (2008) found that trust propensity predicted participants' post-task trust such that when an aid performed well, individuals with high levels of trust propensity were more likely to place greater trust in the aid. Contrarily, when the aid performed poorly, individuals with low levels of trust propensity were more likely to express greater trust in the aid. These results suggest that individuals with high levels of dispositional trust in automation are more inclined to trust reliable systems, but their trust may decline more substantially following system errors.

Research has also shown associations between several more specific personality traits and trust. In terms of the Big Five personality traits, Szalma and Taylor (2012) found that the trait of neuroticism negatively correlated with agreement with correct automated advice. The researchers found no other associations between personality and agreement with automation. Merritt and Ilgen (2008) showed that extroverts exhibit a greater propensity to trust machines than introverts do. McBride, Carter, and Ntuen (2012) used the Minnesota Multiphasic Personality Inventory (MMPI) to show that nurses with an intuitive personality were more likely to accept diagnoses from an automated decision aid than nurses with a sensing personality. These three studies suggest that operators may be more likely to trust or rely upon automation when they are extraverted, are emotionally stable, and have intuitive rather than sensing personalities.

Overall, the research discussed in this section shows that significant individual differences exist in the disposition of people to trust automated systems. Although some of the variables in this

section can change gradually over time (e.g., cultural values, age, and personality traits), they are generally stable within the course of a single interaction. Dispositional trust therefore creates trust variance across interactions with different operators, given that the situation and automated system do not change. In order to better accommodate the trusting tendencies of diverse operators, system designers should consider implementing features that can adapt to the preferences and tendencies of diverse individuals.

Future research directions. Future research is needed in several areas related to dispositional trust in automation. To date, culture-based research is especially scarce, which is problematic due to the wide diversity of people who use automation on a day-to-day basis. Future studies would do well to examine how individuals from different nationalities, religions, and ethnicities tend to trust and utilize automated systems. Along the same lines, more research is needed on the influence of personality traits, especially those that have not yet been studied in the context of automation (i.e., traits that are not assessed by the MMPI or Big Five measures). Future studies could also reassess past findings regarding extraversion, neuroticism, and intuitive versus sensing personalities (McBride et al., 2012; Merritt & Ilgen, 2008; Szalma & Taylor, 2012). For gender, future research should assess how male and female operators respond to specific automation design features, such as communication style and appearance.

The study of age-related changes should be expanded considerably as the use of automation in hospitals, nursing homes, and extended care facilities is now quite common. Past findings regarding age have been somewhat conflicting so future research would do well to systematically examine age differences in trust with different types of automation in multiple, distinct contexts. If possible, researchers should select automated systems that are used frequently by people of varying ages for their studies. Only two of the eight age-related papers identified by this review utilized automated systems that most people could encounter on an everyday basis (Ho et al., 2005; Pak et al., 2012). Additionally, existing studies are limited in that they have involved analyzing differences between only two separate age groups. Future studies might provide new insight by recruiting participants from three or more generational cohorts.

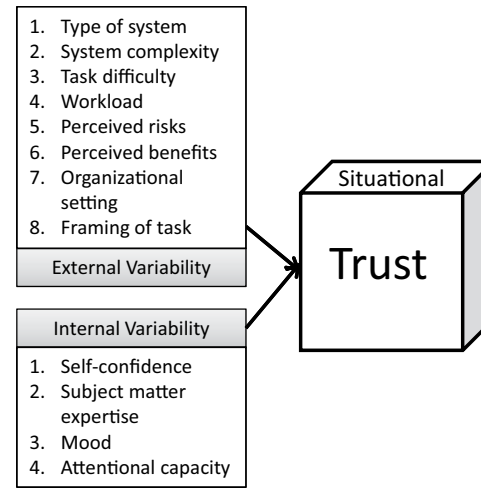

Figure 3. Factors that influence situational trust.

In addition to the variables identified in this review (culture, age, gender, and personality), there are likely other, still unidentified respects in which individual characteristics moderate trusting tendencies with automation. Researchers should continue to explore new dimensions related to dispositional trust in automation, such as the influence of cognitive factors or socioeconomic background. In the next section, we examine situational trust and the context-dependent factors that can alter trust.

Situational Trust

The development of trust, as well as its significance in regard to behavior, varies greatly depending on the situation. (For specific predictions regarding the variability of trust in different contexts, see the trust model proposed by Cohen, Parasuraman, and Freeman, 1998.) Our analysis revealed two broad sources of variability in situational trust: the external environment and the internal, context-dependent characteristics of the operator. The corresponding factors outlined in Figure 3 are important not only because they can directly influence trust but also because they help determine the degree of influence that trust has on behavior toward automation.

External variability. An operator's trust in an automated system depends largely on the type of system, its complexity, and the difficulty of the task for which it is used (e.g., Bailey & Scerbo, 2007; Fan et al., 2008; Madhavan, Wiegmann, & Lacson, 2006; Parkes, 2009; Ross, 2008; Rovira, McGarry, & Parasuraman, 2007; Schwark, Dolgov, Graves, & Hor, 2010; Spain, 2009). Like people, machines have distinct strengths and weaknesses. Human operators take into account the relative difficulty of tasks when evaluating the capabilities of automated systems to complete them (Madhavan et al., 2006). However, problems can arise when operators fail to recognize that a single system can perform inconsistently on two independent tasks or that two systems can perform variably on identical tasks. For example, in one experiment, participants used two decision aids with either mixed reliability or uniform reliability in a video-based search-and-rescue task. Participants rated the trustworthiness of the less reliable aid significantly higher when it was paired with a more reliable aid compared to when it was paired with an aid of the same low reliability (Ross, 2008). This is one example of a perception bias that can occur due to external situational factors (i.e., the presence of another decision aid).

An operator's workload often determines the amount of time and cognition that can be spent monitoring automation. For that reason, workload is a significant variable that can alter the dynamics of human–automation interaction. Empirical research has demonstrated that primary task workload can affect both trusting behaviors (Daly, 2002; McBride et al., 2011; McGarry, 2007; Rajaonah, Tricot, Anceaux, & Millot, 2008) and self-reported trust (Biros, Daly, & Gunsch, 2004; Wetzel, 2005; Willems & Heiney, 2002). In particular, higher workloads appear to have a moderating effect on the positive relationship between trust and reliance (Biros et al., 2004; Daly, 2002; Wetzel, 2005). The reason may be that under high workloads, operators must use automation more often to maintain pace with task demands, regardless of their level of trust (Biros et al., 2004). Other research has shown that certain types of distractors (i.e., visual-spatial and auditory-verbal) can cause reduced trust in automated decision aids, whereas other types of distractors (i.e., visual-verbal and auditory-spatial) can actually increase trust (Phillips & Madhavan, 2011). In one study, however, distractors had no effect on participants' trust in a collision warning system (Lees & Lee, 2007). These conflicting findings suggest that distractors can be influential, but their effect, if any, depends on the degree to which they interfere with system monitoring. If the presence of a distractor causes an operator to overlook an automation error, trust may increase. On the other hand, distractors that do not significantly interfere with system monitoring will likely have no effect on trust or may cause trust to decline slightly (e.g., if automation errors become more salient).

The environment is also important because it helps define the potential risks and benefits associated with the use of automation. Because trust is always relative to an uncertainty, perceptions of risk play a critical role in the development of trust. Perkins, Miller, Hashemi, and Burns (2010) found that participants trusted and used GPS route-planning advice less when situational risk increased through the presence of driving hazards. That finding and other research (Ezer et al., 2008; Rajaonah et al., 2008) suggests that people tend to reduce their reliance on automation when greater risk is involved. However, the reverse effect can occur when the use of automation offers greater benefits and carries fewer potential risks. This can be seen in Lyons and Stokes's (2012) experiment, wherein participants were given assistance from both a human aid and an automated tool in a decision-making task. The researchers discovered that participants relied on the human aid less when making high-risk decisions, suggesting an inclination toward automation.

The inconsistent findings may be attributable to variations in the type and complexity of automation used in the different experiments. Whereas the automated aids that were relied upon less under high-risk conditions provided decision-making advice or controlled actions (Ezer et al., 2008; Perkins et al., 2008; Rajaonah et al., 2008), the automated tool that was relied upon more under high-risk conditions simply displayed information (Lyons & Stokes, 2012).

Thus, the participants in the latter experiment interacted with a more basic form of automation compared to the participants in the former experiments. This finding suggests that under high-risk conditions, operators may have a tendency to reduce their reliance on complex automation but increase their reliance on simple automation.

Trust also depends on the organizational setting of an interaction. For example, trusting behavior toward automated decision aids varies depending on when the system presents its advice (Madhavan & Wiegmann, 2005A) and the operator's degree of personal investment in unaided performance (Beck, McKinney, Dzindolet, & Pierce, 2009). The trust formation process used by individual operators may also vary when multiple teammates share responsibility for monitoring automation. Groups can improve decision making, but they are also subject to certain tendencies, like group polarization, groupthink, and social loafing. Such biases generally limit dissent while promoting conformity. Pairing cognitively diverse operators as teammates may be one method to improve group decision making (Sauer, Felsing, Franke, & Rüttinger, 2006). Further, the culture of a workplace is significant. The opinions and expectations of a single coworker or supervisor can influence other operators' attitudes toward automation. This effect can be seen in a study by Workman (2005), in which social norms regarding the usage of an automated system altered participants' trusting behavior.

Several experiments have demonstrated that the framing of a task can be influential in the trust formation process (Bisantz & Seong, 2001; Huerta et al., 2012; Rice, Trafimow, Clayton, & Hunt, 2008). In one such experiment, different groups of participants were given different reasons for why an automated decision aid might err. One group of participants was told that the aid was subject to sabotage from enemy forces, another group was told that software and hardware failures were common, and the control group was given no information about potential causes for failures. Although the aid's reliability was consistent across groups, the sabotage group ended the experiment with less trust in the aid than the control group did (Bisantz & Seong, 2001). This finding suggests that the presentation of a task can alter the cognitive processes used by operators to evaluate the trustworthiness of automation.

The studies discussed in this section show how external environmental factors can alter the dynamics of human–automation trust. However, external environmental factors are just one part of situational trust; internal variations in factors, such as self-confidence, expertise, mood, and attentional capacity, can also alter situational trust in automation.

Internal variability. Whereas dispositional trust covers the enduring traits of operators, individuals also diverge in more transitory characteristics that depend on context. Self-confidence, which often varies across tasks, is a particularly influential variable that guides trust formation (Lee & See, 2004). It also plays an important role in the decision-making processes associated with control allocation. For example, de Vries, Midden, and Bouwhuis (2003) found that the interaction between trust and self-confidence predicted participants' decisions to perform a route-planning task manually or with assistance from an automated aid. When participants' trust was high and self-confidence low, automation was utilized more frequently. The opposite effect occurred when trust was low and self-confidence high; but overall, participants displayed a slight tendency toward manual control. This finding suggests that when self-confidence and trust are about equal, operators may prefer manual control (de Vries et al., 2003). A more specific aspect of self-confidence is computer self-efficacy, which can be defined as "a judgment of one's ability to use a computer" (Dishaw, Strong, & Bandy, 2002, p. 1023). Research suggests that this variable is positively associated with trust in automation (Madhavan & Phillips, 2010).

Subject matter expertise can also alter trust in automation. Expertise is usually the result of extensive experience in one area and often leads to greater self-confidence. Research has shown that individuals with greater subject matter expertise are less likely to rely on automation than novice operators are (Fan et al., 2008; Sanchez, Rogers, Fisk, & Rovira, 2011). For example, in one experiment, young adults with expe-

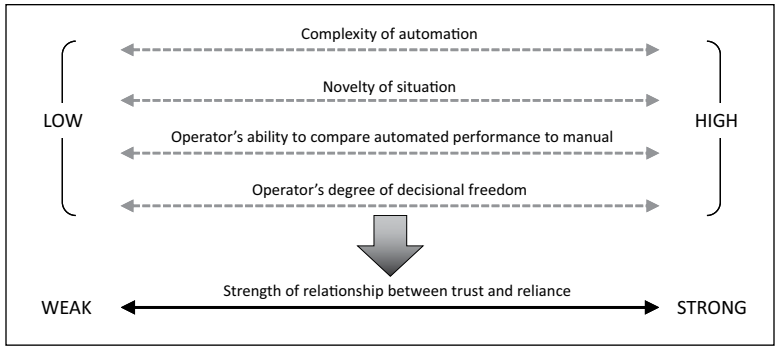

Figure 4. Environmental conditions that are likely to promote stronger relationships between trust and reliance.

rience operating agricultural vehicles were more reluctant to rely on automated alarms during a collision avoidance task than were young adults with little or no agricultural experience (Sanchez, Rogers, Fisk, & Rovira, 2011).

Although subject matter expertise often results from experience, it is not to be confused with experience related to a specific automated system. *Expertise* here refers to an understanding of a specific domain (e.g., operating agricultural vehicles). Knowledge relevant to a specific type of automated system (discussed in the Learned Trust section) can have an entirely different effect on trust and reliance.

Affect is another factor that helps explain why trust develops inconsistently in different contexts. Stokes et al. (2010) found that participants in positive moods expressed higher initial trust in an automated decision aid. Preexisting moods influenced only initial trust in that experiment, but Merritt (2011) found that participants who were implicitly primed to possess the emotion of happiness were more likely to trust an automated weapons detector throughout her experiment. Although the two aforementioned experiments tested different variants of mood and came to slightly different conclusions, they both suggest that an individual's initial emotional state can alter the trust formation process.

A final context-dependent variable related to trust is the attentional capacity of an operator. Attentional capacity often depends on an operator's workload, but other factors, such as motivation, stress, sleep loss, and boredom, can be influential. A recent study by Reichenbach, Onnasch, and Manzey (2011) tested the effects of sleep deprivation on human–automation performance during a supervisory process control task. The researchers found that sleep-deprived participants monitored the automated system more carefully and were less susceptible to automation bias. However, those participants performed worse on a secondary task and were more susceptible to errors when returning to manual control. This finding suggests that although sleep-deprived operators may be able to compensate for their fatigue by monitoring automation more carefully, they are less capable of multitasking when doing so.

To summarize, situational trust in automation depends on both the external environment and the internal, context-dependent characteristics of the human operator. The external factors that can influence trust include system type, system complexity, the task for which a system is used, the potential risks and benefits of using automation, the organizational setting of an interaction, the framing of a task, and the operator's workload. The internal factors that can impact trust include self-confidence, subject matter expertise, mood, and attentional capacity.

Situational factors and the relationship between trust and reliance. In addition to directly influencing trust, situational factors play a leading role in determining the extent to which trust influences behavior toward automation. Lee and See (2004) suggested that trust has a greater impact on reliance when a system's complexity is high and when unplanned events occur that require operators to quickly adapt their behavior. In addition, in the present review, we identified two other environmental conditions that are likely

to increase the positive relationship between trust and reliance. (See Figure 4 for a representation of environmental conditions that may facilitate stronger relationships between trust and reliance.)

First, it seems that trust exerts a greater influence on reliance when the environment provides operators with a greater ability to evaluate the performance of automation relative to unaided manual performance. In other words, subjective trust levels may have a weaker effect on reliance when operators are unable to determine the extent to which automation is actually helping them perform a task. The findings from Spain's (2009) dissertation illustrate this idea. In the experiment, participants used a decision aid that displayed system confidence information while performing a combat identification task with two levels of image quality: high and low. Trust and compliance declined as a function of system confidence in the high–image quality condition but not in the low–image quality condition. Spain attributes this finding to the saliency of automation errors in the different image quality conditions. When the image quality was high, participants reported that it was easier for them to detect targets manually and therefore easier to notice automation errors. When the image quality was low, however, participants had a more difficult time noticing automation errors (Spain, 2009). This study highlights the importance of considering the environment in which a system will be used in order for designers, supervisors, and operators to more effectively facilitate appropriate relationships between trust and reliance.

Decisional freedom is another environmental condition that, when present in higher degrees, likely promotes stronger positive associations between trust and reliance. Decisional freedom represents the extent to which operators are able to make thoughtful decisions about how to best utilize automation. It can be influenced by a variety of situational factors, such as task difficulty, workload, organizational setting, subject matter expertise, mood, and attentional capacity. In general, trust likely has a weaker effect on reliance in the presence of situational factors that inhibit decisional freedom. For example, three studies identified by this review showed that the positive relationship between trust and reliance decreased under higher workloads (Biros et al., 2004; Daly, 2002; Wetzel, 2005). This result may be due to the fact that under high workloads, operators sometimes have little choice but to use automation in order to keep up with task demands (Biros et al., 2004).

Future research directions. There are several areas related to situational trust where existing research is deficient. Future research is needed to confirm the trend identified by this review that under high-risk conditions, operators have a tendency to reduce reliance on complex automation but increase reliance on simple automation. This tendency could be examined by systematically assessing the effects of perceived risks on trust in different types of automation with varying levels of control. Additionally, the existing research on distractors has produced somewhat conflicting results, so researchers should continue to assess how different types of distractors influence trust. In particular, experimental manipulations should focus on the degree to which different distractors interfere with system monitoring and whether or not the attentional interference causes fluctuations in trust.

Future studies could also provide new insight into the context-dependent internal factors that guide trust formation. Specifically, research is needed to confirm the findings of a recent study that suggests that operators may be more likely to monitor automation carefully when they are sleep deprived (Reichenbach et al., 2011). In addition, research could examine the effects of related variables, such as stress, boredom, energy levels, and task motivation.

Researchers should also consider studying individual differences in trust in automation while manipulating situational factors, such as the ones identified in this review. For example, authors of future studies could examine the relationships between specific cultural values or personality traits and trust in situations with variable workloads or levels of risk. Likewise, studies could look at how enduring traits (i.e., dispositional factors) combine with more transitory individual characteristics (i.e., context-dependent situational factors) to guide the trust formation process.

Last, as the use of complex automation continues to spread into more everyday contexts (e.g., smartphones, automobiles, homes, etc.), it

will become increasingly important to study factors that influence human–automation trust in real-world environments. Although experimental manipulations typically become more difficult outside of the laboratory, technology can make up for certain limitations by allowing for more advanced data collection methods. For example, context-aware features of smartphones can be leveraged to passively collect data about an individual's mood, location, activity level, social context, and more (Burns et al., 2011). Technologies such as these could greatly improve existing research methods used to study trust in automation. The next section covers learned trust, which depends on characteristics of the automated system rather than the environment.

Learned Trust

Humans are creatures of experience. Just as people do in interpersonal relationships, operators use knowledge from past interactions with automation when assessing the trustworthiness of novel systems. *Learned trust* represents an operator's evaluations of a system drawn from past experience or the current interaction. This layer of trust is directly influenced by the operator's preexisting knowledge and the automated system's performance. Design features of automation can also impact learned trust, but they do so indirectly, by altering perceptions of system performance.

During the course of an interaction, an automated system may perform variably, and its user's trust will likely fluctuate to correspond with the system's real-time performance. To capture the interactive nature of this relationship, we divide learned trust into two categories: initial and dynamic. Both forms of learned trust are relative to characteristics of the automated system; however, *initial learned trust* represents trust prior to interacting with a system, whereas *dynamic learned trust* represents trust during an interaction. This distinction can be seen in Figure 5, which displays learned trust and its relationship with system reliance.

Another noteworthy feature of Figure 5 is the interdependent relationship between a system's performance, the operator's dynamic learned trust, and his or her reliance on the system. When the performance of an automated system impacts its user's trust, the user's reliance strategy may change. In turn, the user's reliance on the system can affect its performance, thus completing the cycle. (Note the dotted arrows in Figure 5, which represent factors that can change within the course of a single interaction.)

Preexisting knowledge. Before interacting with an automated system, an operator's trust may be biased by the system's reputation. Numerous studies have shown that people display a tendency to trust automation more when it is portrayed as a reputable or "expert" system (de Vries & Midden, 2008; Lerch et al., 1997; Madhavan & Wiegmann, 2007a; Spain, 2009). However, although reputable automation garners more initial trust from operators, this trust may degrade faster when systems make noticeable errors (Madhavan & Wiegmann, 2005b).

Research has also shown that preexisting attitudes and expectations can alter the trust formation process and subsequent usage decisions (Abe & Richardson, 2006; Ezer et al., 2007; Mayer, 2008; Mayer, Sanchez, Fisk, & Rogers, 2006; Merritt, Heimbaugh, LaChapell, & Lee, 2012; Workman, 2005). For example, Merritt et al. (2012) studied the impact of implicit and explicit attitudes toward automation on trust in an automated weapons detector that performed variably across three conditions (clearly good, ambiguous, and clearly bad). Implicit attitudes differ from explicit attitudes in that they function purely through associations, and people are not usually aware of them (Merritt et al., 2012). In their experiment, Merritt et al. found that the interaction between implicit and explicit attitudes had an additive effect on trust in the ambiguous and clearly bad conditions. When both implicit and explicit attitudes toward automation were positive, participants were more likely to express greater trust in the aid. This finding provides evidence of an unconscious mechanism that guides the formation of trust in automation. However, because research in this area is limited, future studies are needed to further examine the role of implicit attitudes in guiding human–automation interaction.

Past experience with an automated system, or a similar technology, can significantly alter the trust formation process. However, to understand the specific effect that experience has on

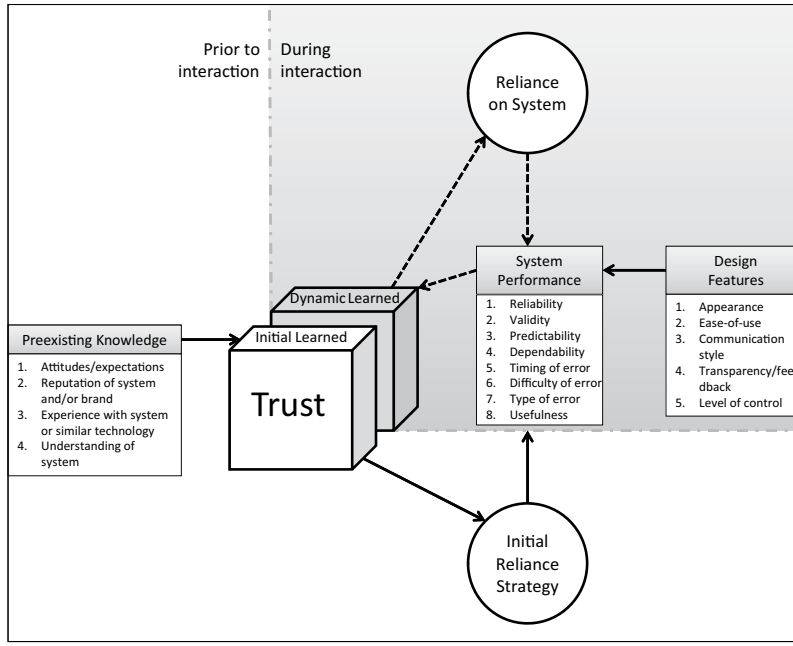

Figure 5. Factors that influence learned trust. The dotted arrows represent factors that can change within the course of a single interaction.

trust, one must distinguish between subject matter expertise (related to situational trust) and past experience with automation (related to learned trust). An illustration of this distinction arises from comparing the findings of two experiments focused on the effect of past experience on trust in automation. In the first study, Yuliver-Gavish and Gopher (2011) found that participants relied on a decision support system more after they gained experience using the system. At first, this result may seem to oppose the findings of Sanchez et al. (2011), who found that experienced farmers relied less on automation during a collision avoidance task (with an agricultural vehicle) than participants with no farming experience. However, unlike the experienced participants in Yuliver-Gavish and Gopher's study, the experienced participants in Sanchez et al.'s study had never before operated the specific type of automated alarm system used during the collision avoidance task. Thus, the type of experience studied in Sanchez et al.'s experiment is better classified as a situational factor rather than a learned factor. This distinction may help explain why past experience led to reduced reliance in Sanchez et al.'s study but increased reliance in Yuliver-Gavish and Gopher's experiment.

Although Yuliver-Gavish and Gopher's (2011) study and several other experiments indicate that past experience with automation (Manzey, Reichenbach, & Onnasch, 2012; Riley, 1996) or similar technology (e.g., video games; see Cummings, Clare, & Hart, 2010) provides operators with a greater tendency to trust or rely upon automation, other research has shown that this is not always the case (Bailey & Scerbo, 2007). In fact, the opposite trend can occur if an operator's past involvement with an automated system was unproductive. Manzey et al. (2012) showed that negative past experiences led to reduced trust in an automated fault identification system. Regardless of its specific effect, past experience almost always plays a role in guiding human–automation interaction. Experience is also significant because it can enhance an operator's understanding of an automated system's purpose and process.

Opinions and knowledge about the purpose and process of automated systems help guide the trust formation process. When operators lack knowledge about the purpose of a system or how

it functions, they will likely have a more difficult time accurately aligning their trust to a system's real-time reliability. This is particularly true when situational factors help determine a system's performance. For example, the trust formation process used by operators depends on the extent to which they understand how the performance of automation varies in distinct contexts and at different temporal phases (Cohen et al., 1998). Misperceptions about these variables can lead to misuse, disuse, and/or abuse of automation. Training is one way to reduce the likelihood of these behaviors. Research has shown that by training operators about an aid's actual reliability, it is possible to alter trust and reliance patterns (Cassidy, 2009; Koustanaï, Cavallo, Delhomme, & Mas, 2012; Masalonis, 2003), facilitate better task performance (Koustanaï et al., 2012; Wilkison, 2008), and reduce complacency (Manzey, Bahner, & Hueper, 2006). In addition to training, several studies have shown that decision aids designed to supplement their decision making with real-time confidence levels help users calibrate their trust appropriately (Antifakos, Kern, Schiele, & Schwaninger, 2005; McGuirl & Sarter, 2006). Although system confidence information does not explicitly reveal anything about purpose or process, it reminds operators that automation is imperfect and can provide only a "best guess" based on the information available in a given situation.

The variables discussed in this section can bias operators' trust before any interaction with a system has occurred. Because preexisting knowledge does not usually change in the course of a single interaction, it impacts only initial learned trust, not dynamic learned trust. Once an operator begins interacting with a system, its performance can impact dynamic learned trust, which can change drastically over the course of an interaction. However, perceptions of performance depend largely on the manner in which information is presented to an operator. Thus, the design features of automation are significant, because they can indirectly influence trust by altering perceptions of system performance.

Design features. Substantial research has shown that design features can alter trust in automation. The appearance of automation is one important consideration. Computer interfaces are often the primary visual component of systems. When this is the case, interfaces must be thoughtfully arranged. Several e-commerce studies have shown that aesthetically pleasing websites are trusted more than less attractive sites (Kim & Moon, 1998; Li & Yeh, 2010; Wakefield, Stocks, & Wilder, 2004). Those findings prompted Weinstock, Oron-Gilad, and Parmet (2012) to test the effect of system aesthetics on trust in an in-vehicle automated system. On the basis of inconclusive results, Weinstock et al. suggested that aesthetic design may be less relevant to trust in automation than to trust in e-commerce websites.

Nevertheless, other research suggests that the anthropomorphism of an interface can be a significant variable (de Visser et al., 2012; Gong, 2008; Green, 2010; Pak et al., 2012). For example, a recent study showed that adding a picture of a physician to the interface of a diabetes management application led younger participants to place greater trust in the system's advice (Pak et al., 2012). Additionally, de Visser et al. (2012) found that increasing the anthropomorphism of an automated aid caused participants to exhibit greater trust resilience (i.e., their trust declined less rapidly) following system errors. Taken together, these findings suggest that increasing the humanness of systems may help reduce automation disuse with certain types of automation. However, designers must consider the expected characteristics of potential users (e.g., age, gender, culture), as anthropomorphizing an interface can impact the trust formation process differently for diverse individuals (Pak et al., 2012).

The ease of use of a system must also be taken into account. Numerous e-commerce studies have shown a positive relationship between the ease of use of a website and consumer trust (e.g., Gefen et al., 2003; Li & Yeh, 2010; Ou & Sia, 2010; Zhou, 2011). On the other hand, surprisingly few researchers have studied this variable in the context of automation. Atoyan, Duquet, and Robert (2006) showed that trust ratings of an intelligent data fusion system increased as the usability of the system improved through "giving better traceability of the results, enhanced visual clarity, and effective feedback"

(p. 120). The findings of this study are limited, however, in that there were only six participants. Wang, Jamieson, and Hollands (2011) may have indirectly studied ease of use by assessing the impact of design features on trust in a combat identification aid. The researchers found that participants trusted the aid's unknown feedback more when it was displayed explicitly rather than implicitly. This finding suggests that increasing the saliency of automated feedback can promote greater trust.

Automated systems can communicate with their users in a variety of ways. Different modes of communication can lead operators to incongruent levels of trust in automation. For example, some automated systems utilize verbal communication from embodied computer agents, rather than basic text, in order to provoke feelings of human–human trust. However, research has revealed that people sometimes prefer text interfaces over anthropomorphic agents (Gong, 2008). In order to promote trust, embodied computer agents must be carefully constructed to appear both anthropomorphic and trustworthy (Gong, 2008). Results from one study suggest that a computer agent's eye movement, normality of form, and chin shape are important variables that can impact trust (Green, 2010). Additionally, the gender of a computer agent can be influential. E. J. Lee (2008) found that participants complied more with male computer agents communicating via text than with female agents. Overall, this body of research suggests that an automated system's communication style can be an important variable. In order to promote appropriate trust in automation, designers should choose a mode of communication that corresponds to the actual capabilities of a system.

Within a given mode of communication, automated systems can exhibit a wide range of distinct "personalities." Research has shown that certain artificially assigned traits can bias operators' trust. For example, Parasuraman and Miller (2004) found that instilling automation with good etiquette, operationally defined as "a communication style that was 'non-interruptive' and 'patient,'" led to greater trust and improved diagnostic performance (p. 54). In a later study, Spain and Madhavan (2009) defined automation etiquette as "politeness." By manipulating word choice alone, the researchers elicited different levels of subjective trust in an automated aid. These findings demonstrate the role of "automation personality" in guiding operators' trust development.

Another influential variable is the transparency of automation. *Transparency* refers to the degree to which "the inner workings or logic [used by] the automated systems are known to human operators to assist their understanding about the system" (Seong & Bisantz, 2008, p. 611). Numerous studies have shown that designing systems that provide users with accurate feedback about their reliability or how they operate can better facilitate appropriate trust (Dadashi, Stedmon, & Pridmore, 2012; Gao & Lee, 2006; Jamieson, Wang, & Neyedli, 2008; Seong & Bisantz, 2008; Wang, Jamieson, & Hollands, 2009) and improve human–automation task performance (Bagheri & Jamieson, 2004; Bass, Baumgart, & Shepley, 2013; Bean, Rice, & Keller, 2011; Beck, Dzindolet, & Pierce, 2007; Dzindolet, Pierce, Peterson, Purcell, & Beck, 2002; Oduor & Wiebe, 2008; Seppelt & Lee, 2007). For example, Seong and Bisantz (2008) found that providing participants with cognitive feedback from a system (in the form of meta-information) led to higher trust ratings in low-reliability automation but lower trust ratings in high-reliability automation. The authors attribute this outcome to the meta-information's effect of helping operators in the low-reliability condition ignore the aid when appropriate and reminding the operators in the high-reliability condition that the aid was imperfect (Seong & Bisantz, 2008).

In a similar study, Wang et al. (2009) found that providing operators with system reliability information can improve the appropriateness of trust. However, displaying this information in different ways can alter reliance strategies and human-automation performance (Lacson, Wiegmann, & Madhavan, 2005; Neyedli, Hollands, & Jamieson, 2011). Finally, Dzindolet et al. (2003) showed that providing operators with explanations of why automation failures occur can lead to increased trust. Overall, this research suggests that designing transparent systems that provide accurate, useful feedback can reduce the frequency of automation misuse and disuse.

Trust in automation also depends on the level of control the operator has over automated functions (de Visser & Parasuraman, 2011; Rovira et al., 2007; Verberne, Ham, & Midden, 2012; Willems & Heiney, 2002). For example, a recent study showed that automation that takes over functions while providing information to the operator (~Level 7 automation) is perceived as more trustworthy than automation that takes over functions without providing any information to the operator (~Level 10 automation) (Verberne et al., 2012). This finding suggests that operators may have a tendency to trust lower levels of complex automation more than higher levels. Unfortunately, low-level automation often decreases efficiency through the added delays that arise when a system provides information to its operator and then waits for input. Still, although high-level automation can perform tasks quicker, human operators are taken "out of the loop." This result means that operators cannot prevent errors in systems, so instead, they must be addressed after they occur. Additionally, operators who are taken out of the loop may become dependent on automation to perform tasks, and if failures occur, they will likely have a more difficult time completing tasks manually. In order to determine an optimal level of control, designers should consider the potential demands of the environment in which a system will likely be used.

In certain environments, adaptive automation can be an effective solution to the trade-off regarding different levels of control. Adaptive automation offers the potential to improve both the safety and efficiency of human–automation work systems by adapting its level of control to match the needs of the current situation (de Visser & Parasuraman, 2011; Kaber & Endsley, 2004). Adaptive automation can also be useful because it can alter its behavior based on the preferences of the user. For example, research suggests that operators with different levels of attentional control may prefer distinct levels of automation (Thropp, 2006). In spite of the potential benefits, adaptive automation is not always practical for use in the real world.

In the present review, we identified five major design features that must be carefully considered: appearance, ease of use, communication style, transparency, and level of control. Table 3 presents specific design recommendations for each of these features based on the research discussed in this section. Readers with an interest in design are encouraged to revisit Lee and See's (2004) review for more design principles.

Performance. Trust depends on results. Substantial research has shown that human operators adjust their trust in automation to reflect its real-time performance. Several different aspects of performance have been studied. First, numerous studies have shown that the reliability and validity of an automated system's functions are important antecedents of trust (Bailey & Scerbo, 2007; de Visser & Parasuraman, 2011; Madhavan & Wiegmann, 2007a; Oduor & Campbell, 2007; Seong & Bisantz, 2008; Ross, 2008; Ross, Szalma, Hancock, Barnett, & Taylor, 2008; Sanchez et al., 2004; Wetzel, 2005). *Reliability* refers to the consistency of an automated system's functions, and *validity* refers to the degree to which an automated system performs the intended task. The predictability and dependability of automation are also important. *Predictability* refers to the extent to which automation performs in a manner consistent with the operator's expectations, and *dependability* refers to the frequency of automation breakdowns or error messages (Merritt & Ilgen, 2008). Research has shown that operators trust automated systems more when they are highly predictable and dependable (Biros et al., 2004; Merritt & Ilgen, 2008).

When automation failures occur, distinct error types can have different effects on trust and subsequent trusting behaviors. In particular, research has shown that *false alarms* (when systems incorrectly alert operators to the presence of a signal) and *misses* (when automation fails to detect a true signal) generally have different effects on trust-dependent behaviors (Sanchez, 2006). Importantly, false alarms call for compliance (operators must assume that a signal is present), whereas misses require reliance (operators must assume that a signal is absent). This distinction is significant because numerous studies have found that false-alarm-prone automation reduces operator compliance more than reliance, whereas miss-prone automation reduces reliance more than compliance (Davenport &

TABLE 3: Design Recommendations for Creating Trustworthy Automation

Design Feature	Design Recommendation	Source of Empirical Support
Appearance/ anthropomorphism	Increase the anthropomorphism of automation in order to promote greater trust	de Visser et al. (2012); Pak, Fink, Price, Bass, & Sturre (2012)
	Consider the expected age, gender, culture, and personality of potential users because anthropomorphic design features may impact trust differently for diverse individuals	Lee (2008)[a]; Pak et al. (2012)
Ease of use	Simplify interfaces and make automation easy to use to promote greater trust	Atoyan, Duquet, & Robert (2006); Gefen, Karahanna, & Straub (2003)[b]; Li & Yeh (2010)[b]; Ou & Sia (2010)[b]; Zhou (2011)**
	Consider increasing the saliency of automation feedback to promote greater trust	Wang, Jamieson, & Hollands (2011)
Communication style	Consider the gender, eye movements, normality of form, and chin shape of embodied computer agents to ensure an appearance of trustworthiness	Gong (2008)[a]; Green (2010)[a]; Lee (2008)[a]
	Increase the politeness of an automated system's communication style to promote greater trust	Parasuraman & Miller (2004); Spain & Madhavan (2009)
Transparency/ feedback	Provide users with accurate, ongoing feedback concerning the reliability of automation and the situational factors that can affect its reliability in order to promote appropriate trust and improve task performance	Bagheri & Jamieson (2004); Bass, Baumgart, & Shepley (2013); Bean, Rice, & Keller (2011); Beck, Dzindolet, & Pierce (2007); Dadashi, Stedmon, & Pridmore (2012); Dzindolet, Pierce, Peterson, Purcell, & Beck (2002); Dzindolet, Peterson, Pomranky, Pierce, & Beck (2003); Gao & Lee (2006); Jamieson, Wang, & Neyedli (2008); Oduor & Wiebe (2008); Seong & Bisantz (2008); Seppelt & Lee (2007); Wang, Jamieson, & Hollands (2009)
	Evaluate tendencies in how users interpret system reliability information displayed in different formats	Lacson, Wiegmann, & Madhavan (2005); Neyedli, Hollands, & Jamieson (2011)
	Consider providing operators with additional explanations for automation errors that occur early in the course of an interaction or on tasks likely to be perceived as "easy" in order to discourage automation disuse	Madhavan, Wiegmann, & Lacson, 2006; Manzey, Reichenbach, & Onnasch, 2012; Sanchez, 2006
Level of control	Consider increasing the transparency of high-level automation to promote greater trust	Verberne, Ham, & Midden (2012)
	Evaluate user preferences for levels of control based on psychological characteristics	Thropp (2006)

[a]Indicates study on trust in embodied computer agents.
[b]Indicates study on trust in websites.

Bustamante, 2010; Dixon, 2007; Dixon & Wickens, 2006; Levinthal & Wickens, 2006; Rice, 2009). It is important to note, however, that compliance and reliance are not completely independent of each other (Dixon, Wickens, & McCarley, 2007).

In addition to their distinctive influences on trust-dependent behavior, false alarms and misses may affect subjective feelings of trust differently. One potential reason for this is that false alarms are usually more salient than misses and require the operator to put effort into unnecessary investigations. As a result, false alarms may have a greater negative impact on trust than misses. Although some research has supported this hypothesis (Johnson, 2004), other research suggests that false alarms and misses have similar effects (Madhavan et al., 2006; Rovira & Parasuraman, 2010). Additionally, at least two studies have shown that participants trusted false-alarm-prone automation more than miss-prone automation (Davenport & Bustamante, 2010; Stanton, Ragsdale, & Bustamante, 2009). Overall, the specific impact that false alarms and misses have on trust likely depends on the negative consequences associated with each error type in a specific context. For example, whereas a false alarm from a carbon monoxide detector is a minor inconvenience, a miss can result in death. In this case, misses will likely cause greater damage to trust than false alarms will. The relative influence of other types of automation failures, such as breakdowns and error messages, has yet to be determined.

The negative effect that automation errors have on trust also depends on the timing of the error and the relative difficulty associated with the error. Research has shown that automation errors that occur early in the course of an interaction have a greater negative impact on trust than errors occurring later (Manzey et al., 2012; Sanchez, 2006). This finding suggests that first impressions with automation are important, and early errors can have a lasting impact on the trust formation process. This impact may be particularly true in dealings with unfamiliar automation, because a system's initial performance is the primary basis for trust. In addition, automation failures on tasks perceived as easy have a greater negative impact on trust than errors on tasks perceived as difficult (Madhavan et al., 2006). Human operators may be less willing to trust automation after "easy" failures because of an assumption that machines and humans process information in similar ways. Thus, operators may assume that if an automated system is incapable of performing a seemingly basic function, it will not be able to perform complex tasks either. In order to prevent automation disuse stemming from early or "easy" automation errors, system designers should consider providing operators with additional feedback after these types of errors occur.

The usefulness of an automated system is the final performance-based variable that can influence trust. Trust in automation is always relative to a task that the operator wants performed. If an operator realizes that using automation to perform a task actually makes the task more arduous, he or she will likely see no need to use and therefore trust automation. Thus, automation must first prove itself useful to operators in order for trust to be at stake. Few authors of empirical research have studied usefulness directly. However, Parkes (2009) found that participants relied more on advice from a decision support system when they perceived it as useful. Additionally, in two separate studies, Abe and Richardson (2004, 2006) showed that drivers trusted a collision warning system significantly less when the system provided alarms after braking had already been initiated. The reduction in trust may have been the result of the late alarms' providing weaker benefits to drivers.

The research discussed in this section shows how operators adjust their trust in automation to correspond to its ongoing performance. Although trust is largely dependent on performance, the trust formation process also depends on situational factors, the design features of automation, the operator's dispositional trust, and preexisting knowledge. Within the context of a single interaction, most of those variables are stable, whereas performance is not.

This distinction can be seen in both Figure 5 and Figure 6, wherein initial learned trust represents trust factors that do not change within a single interaction, whereas dynamic learned trust reflects the variable nature of trust. An operator's initial learned trust helps determine

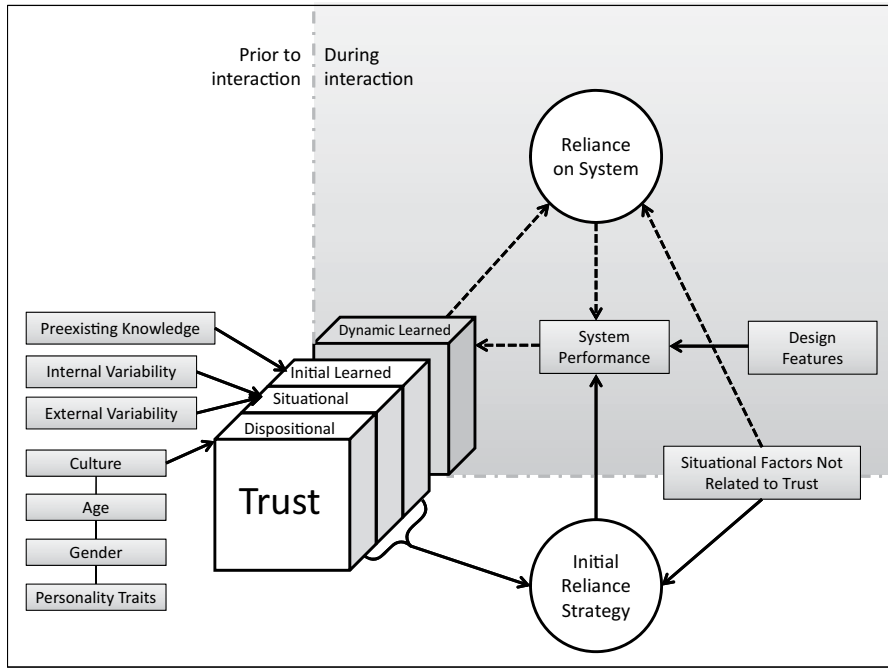

Figure 6. Full model of factors that influence trust in automation. The dotted arrows represent factors that can change within the course of a single interaction.

his or her initial reliance strategy. The degree to which a system is initially relied upon can affect its subsequent performance. The performance of a system can then impact its operator's dynamic learned trust. If this occurs, the operator's reliance strategy may change, which will likely affect the system's future performance. This interdependent relationship exemplifies the dynamic nature of trust in automation.

Situational factors not related to trust. Although both initial and dynamic learned trust influence reliance on automation, they are not the only contributing factors. Lee and See (2004) explain, "Trust guides—but does not completely determine—reliance" (p. 51). Additional situational factors, such as the level of effort required to engage a system, the alternatives to using automation, time constraints, and the operator's situational awareness and physical well-being, can guide reliance without necessarily impacting trust. For example, Rice and Keller (2009) showed that participants were more likely to comply with a diagnostic aid when their decision time was reduced. Thus, an operator's degree of decisional freedom, as well as other situational factors, can sway the undercurrents of the interdependent relationship among trust, reliance, and performance.

Future research directions. Although authors of considerable research have studied factors related to learned trust, there are numerous areas where future studies can build on existing knowledge and provide new insight. For preexisting knowledge, more research is needed to discern the relative influence that different types of past experience have on trust and reliance. In the present review, we identified the discrepancy between domain experience (a situational trust factor) and system experience (a learned trust factor) to be an important distinction, but researchers have yet to examine the effects of other types of past experience (e.g., positive vs. negative experience) in much detail. Additionally, scarce research has shown how cultural differences in expectations and knowledge regarding automation can impact trust and reliance behaviors.

There are several areas related to design where existing research is lacking. In the present review, we identified 33 studies in which design features were experimentally manipulated, but

only 4 of these studies utilized automated systems that most people might encounter on a day-to-day basis, independent of their occupation (Pak et al., 2012; Seppelt & Lee, 2007; Verberne et al., 2012; Weinstock et al., 2012). In contrast, 18 of these studies utilized combat or target identification aids. This trend is noteworthy because complex automated systems with critical functionalities are becoming increasingly relied upon outside of work settings. Authors of future studies should address this transition by examining the design implications of more diverse automation, such as medical technology, smart home interfaces, and information management systems.

Additionally, more research is needed on the impact of system aesthetics on trust in automation. Although aesthetics have been shown to be quite influential in promoting trust in e-commerce websites (Kim & Moon, 1998; Li & Yeh, 2010; Wakefield et al., 2004), the only researchers who looked at this variable in the context of route-planning automation did not find any significant effects (Weinstock et al., 2012). Likewise, e-commerce research suggests that ease of use could be influential in guiding operators' trust in automated systems (Gefen et al., 2003; Li & Yeh, 2010; Ou & Sia, 2010; Zhou, 2011), but the only researchers who directly looked at this variable in the context of automation had only six participants (Atoyan et al., 2006). In addition, future studies are needed to determine how design features interact with dispositional factors (e.g., age, culture, gender, and personality) to guide the trust formation process. Researchers should consider evaluating tendencies in how diverse individuals trust automated systems with different communication styles, degrees of anthropomorphism, and levels of control. Expanding this type of research is crucial in order to aid designers in building more adaptable systems that can alter their behavior based on user preferences.

Future studies are also needed to provide new insight into the interdependent relationships between operator trust, operator reliance, and system performance. In particular, researchers should look at factors that affect the strength of these relationships. Findings from the present review suggest that trust and reliance are more strongly positively correlated when operators have greater decisional freedom and when information about an automated system's performance relative to unaided manual performance is available for a given task.

Researchers should also consider studying how operators naturally react to preplanned automation breakdowns and error messages because these types of failures have yet to be studied in much detail. Most of the existing research on error types has focused on the differential effects of automation false alarms and automation misses on trust, reliance, and compliance. In the present review, we identified 12 studies on this topic, but a consistent trend regarding the relative influence of false alarms versus misses on trust was not found. Rather, it seems that the degree of influence depends on the consequences of each error type in a given environment. Authors of future studies could investigate this hypothesis further by systematically manipulating the negative consequences of false alarms versus misses in multiple experimental tasks.

CONCLUSION

The purpose of this paper was to review and synthesize findings from recent research on human–automation trust and reliance. Through a systematic review process of academic literature from January 2002 through June 2013, we identified 101 empirical papers on the topic, consisting of 127 separate studies. Our analysis led to the construction of a model that conceptualizes the various factors that influence trust and reliance using a layered approach. As displayed in the model (see Figure 6), the complexities of trust can be reduced to three broad layers of variability: dispositional trust, situational trust, and learned trust. Distinct factors influence each layer, but any given operator's trust in an automated system is a compilation of the operator's trusting tendencies, the situation, and the operator's perceptions of the system. This framework can serve as a useful guide for future research into the intricacies of trust in automation. It can also be applied to help develop training interventions and design procedures that encourage appropriate trust. (See Table 3 for specific design recommendations.)

Although trust is a particularly influential variable that guides human reliance on automation, its degree of influence depends on a number of situational factors. For example, findings from the present review suggest that trust may carry less meaning in situations where operators have minimal decisional freedom or are unable to effectively compare the performance of automation to unaided manual performance. Additionally, trust tends to have less of an effect on reliance in anticipated situations and when operators are able to fully understand automation (Lee & See, 2004). These environmental conditions are important to consider in order to more accurately gauge the extent to which an operator's trust in an automation system will affect his or her reliance on the system in a specific setting. (See Figure 4 for a representation of these environmental conditions.)

Due to the wide variety of experimental paradigms included in this analysis, it is rather difficult to hypothesize about the relative influence that each layer has on trust in automation. However, a recent meta-analysis of factors that affect trust in human–robot interactions offers some insight. Hancock et al. (2011) quantitatively examined the relative weight of human, environmental, and robot-related factors that influence human–robot trust. In their meta-analysis of 11 experimental studies, the authors found trust to be most influenced by characteristics of the robot, followed by characteristics of the environment. Human-related trust factors were found to be the least significant, but the authors attributed this finding to the shortage of experiments focused on individual differences. In the context of automation, research on dispositional trust is also somewhat scarce compared to research on situational and learned trust. Nevertheless, the existing research on dispositional trust is vast enough to show that individual differences are important to consider and should be the focus of more research in the coming years. More specific directions for future research on dispositional trust, as well as situational and learned trust, are discussed at the end of each corresponding subsection.

Automation offers tremendous potential to improve the safety and efficiency of countless processes. Already, humans rely on the proper functioning of numerous automated systems on a day-to-day basis. This dependency is constantly increasing and will only grow further in the coming years as our society becomes increasingly modernized. In order to promote the proper use of automation and minimize the frequency of related accidents, trust formation should be viewed as a dynamic process guided by a complex interaction of factors stemming from three interdependent layers of variability: dispositional trust, situational trust, and learned trust.

KEY POINTS

- Recent empirical research on factors that influence trust in automation was systematically reviewed, leading to the construction of a trust model based on three interdependent layers of variability (dispositional trust, situational trust, and learned trust).
- Designers can better facilitate appropriate trust by providing users with ongoing feedback concerning the reliability of automation and the situational factors that affect its performance.
- In order to promote greater trust and discourage automation disuse, designers should consider increasing an automated system's degree of anthropomorphism, transparency, politeness, and ease of use.
- The strength of the relationship between trust and reliance depends on the complexity of automation, the novelty of the situation, the operator's ability to compare manual to automated performance, and the operator's degree of decisional freedom.
- Future research directions are suggested for each trust layer based on gaps, trends, and patterns found in existing research.

REFERENCES

Abe, G., & Richardson, J. (2004). The effect of alarm timing on driver behaviour: An investigation of differences in driver trust and response to alarms according to alarm timing. *Transportation Research Part F: Traffic Psychology and Behaviour*, *7*, 307–322.

Abe, G., & Richardson, J. (2006). Alarm timing, trust and driver expectation for forward collision warning systems. *Applied Ergonomics*, *37*, 577–586.

Antifakos, S., Kern, N., Schiele, B., & Schwaninger, A. (2005). Towards improving trust in context-aware systems by displaying system confidence. In *Proceedings of Mobile HCI 2005* (pp. 9–14). New York, NY: ACM.

Atoyan, H., Duquet, J. R., & Robert, J. M. (2006). Trust in new decision aid systems. *Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine* (pp. 115–122). New York, NY: ACM.

Bagheri, N., & Jamieson, G. A. (2004). The impact of context-related reliability on automation failure detection and scanning behaviour. *2004 IEEE International Conference on Systems, Man and Cybernetics*, *1*, 212–217.

Bailey, N. R., & Scerbo, M. W. (2007). Automation-induced complacency for monitoring highly reliable systems: The role of task complexity, system experience, and operator trust. *Theoretical Issues in Ergonomics Science*, *8*, 321–348.

Barber, B. (1983). *The logic and limits of trust*. New Brunswick, NJ: Rutgers University Press.

Bass, E. J., Baumgart, L. A., & Shepley, K. K. (2013). The effect of information analysis automation display content on human judgment performance in noisy environments. *Journal of Cognitive Engineering and Decision Making*, *7*, 49–65.

Bean, N. H., Rice, S. C., & Keller, M. D. (2011). The effect of gestalt psychology on the system-wide trust strategy in automation. In *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting* (pp. 1417–1421). Santa Monica, CA: Human Factors and Ergonomics Society.

Beck, H. P., Dzindolet, M. T., & Pierce, L. G. (2007). Automation usage decisions: Controlling intent and appraisal errors in a target detection task. *Human Factors*, *49*, 429–437.

Beck, H. P., McKinney, J. B., Dzindolet, M. T., & Pierce, L. G. (2009). Effects of human-machine competition on intent errors in a target detection task. *Human Factors*, *51*, 477–486.

Biros, D. P., Daly, M., & Gunsch, G. (2004). The influence of task load and automation trust on deception detection. *Group Decision and Negotiation*, *13*, 173–189.

Biros, D. P., Fields, G., & Gunsch, G. (2003). The effect of external safeguards on human-information system trust in an information warfare environment. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, 10. New York, NY: IEEE (pp. 1–10).

Bisantz, A. M., & Seong, Y. (2001). Assessment of operator trust in and utilization of automated decision-aids under different framing conditions. *International Journal of Industrial Ergonomics*, *28*, 85–97.

Burns, M. N., Begale, M., Duffecy, J., Gergle, D., Karr, C. J., Giangrande, E., & Mohr, D. C. (2011). Harnessing context sensing to develop a mobile intervention for depression. *Journal of Medical Internet Research*, *13*(3), e55.

Cassidy, A. M. (2009). *Mental models, trust, and reliance: Exploring the effect of human perceptions on automation use*. (Unpublished Masters Thesis). Naval Postgraduate School, Monterey CA.

Cohen, M. S., Parasuraman, R., & Freeman, J. (1998). *Trust in decision aids: A model and a training strategy*. Paper presented at the Command and Control Research and Technology Symposium, Washington, DC.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*, 909–927.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*, 737–758.

Cummings, M. L., Clare, A., & Hart, C. (2010). The role of human-automation consensus in multiple unmanned vehicle scheduling. *Human Factors*, *52*, 17–27.

Czaja, S. J., & Sharit, J. (1998). Age differences in attitudes toward computers. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *53*, 329–340.

Dadashi, N., Stedmon, A. W., & Pridmore, T. P. (2012). Semi-automated CCTV surveillance: The effects of system confidence, system accuracy and task complexity on operator vigilance, reliance and workload. *Applied Ergonomics*, *44*, 730–738.

Daly, M. A. (2002). *Task load and automation use in an uncertain environment* (Master's thesis). Retrieved from ProQuest Dissertations and Theses.

Davenport, R. B., & Bustamante, E. A. (2010). Effects of false-alarm vs. miss-prone automation and likelihood alarm technology on trust, reliance, and compliance in a miss-prone task. In *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting* (pp. 1513–1517). Santa Monica, CA: Human Factors and Ergonomics Society.

de Visser, E. J., Krueger, F., McKnight, P., Scheid, S., Smith, M., Chalk, S., & Parasuraman, R. (2012). The world is not enough: Trust in cognitive agents. In *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting* (pp. 263–267). Santa Monica, CA: Human Factors and Ergonomics Society.

de Visser, E. J., & Parasuraman, R. (2011). Adaptive aiding of human-robot teaming effects of imperfect automation on performance, trust, and workload. *Journal of Cognitive Engineering and Decision Making*, *5*, 209–231.

de Vries, P., & Midden, C. (2008). Effect of indirect information on system trust and control allocation. *Behaviour & Information Technology*, *27*, 17–29.

de Vries, P., Midden, C., & Bouwhuis, D. (2003). The effects of errors on system trust, self-confidence, and the allocation of control in route planning. *International Journal of Human-Computer Studies*, *58*, 719–735.

Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations*, *13*, 123–139.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, *34*, 373–396.

Dishaw, M. T., Strong, D. M., & Bandy, D. B. (2002, August). *Extending the task-technology fit model with self-efficacy constructs*. Paper presented at the Eighth Americas Conference on Information Systems (pp. 1021–1027), Dallas, Texas.

Dixon, S. R. (2007). *Imperfect diagnostic automation: How adjusting bias and saliency affects operator trust* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.

Dixon, S. R., & Wickens, C. D. (2006). Automation reliability in unmanned aerial vehicle control: A reliance-compliance model of automation dependence in high workload. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *48*(3), 474–486.

Dixon, S. R., Wickens, C. D., & McCarley, J. S. (2007). On the independence of compliance and reliance: Are automation false alarms worse than misses? *Human Factors*, *49*, 564–572.

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The role of trust in automation reliance. *International Journal of Human–Computer Studies*, *58*, 697–718.

Dzindolet, M., Pierce, L., Peterson, S., Purcell, L., & Beck, H. (2002). The influence of feedback on automation use, misuse, and disuse. In *Proceedings of the Human Factors and Ergonomics Society 46th Annual Meeting* (pp. 551–555). Santa Monica, CA: Human Factors and Ergonomics Society.

Engell, A. D., Haxby, J. V., & Todorov, A. (2007). Implicit trustworthiness decisions: Automatic coding of face properties in human amygdala. *Journal of Cognitive Neuroscience*, *19*, 1508–1519.

Ezer, N., Fisk, A. D., & Rogers, W. A. (2007). Reliance on automation as a function of expectation of reliability, cost of verification, and age. In *Proceedings of the Human Factors and Ergonomics Society 51st Annual Meeting* (pp. 6–10). Santa Monica, CA: Human Factors and Ergonomics Society.

Ezer, N., Fisk, A. D., & Rogers, W. A. (2008). Age-related differences in reliance behavior attributable to costs within a human-decision aid system. *Human Factors*, *50*, 853–863.

Fan, X., Oh, S., McNeese, M., Yen, J., Cuevas, H., Strater, L., & Endsley, M. R. (2008). The influence of agent reliability on trust in human-agent collaboration. In *Proceedings of the 15th European Conference on Cognitive Ergonomics: The Ergonomics of Cool Interaction* (Article 7). New York, NY: ACM.

Faulty reading helped cause Dutch plane crash. (2009, March 4). *CNN Europe*. Retrieved from http://www.cnn.com/2009/WORLD/europe/03/04/plane.crash/index.html?iref=allsearch

Gao, J., & Lee, J. D. (2006, October). Effect of shared information on trust and reliance in a demand forecasting task. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting* (pp. 215–219). Santa Monica, CA: Human Factors and Ergonomics Society.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*, 51–90.

Gong, L. (2008). How social is social responses to computers? The function of the degree of anthropomorphism in computer representations. *Computers in Human Behavior*, *24*, 1494–1509.

Green, B. D. (2010). *Applying human characteristics of trust to animated anthropomorphic software agents* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.

Hancock, P. A., Billings, D. R., Oleson, K. E., Chen, J. Y. C., de Visser, E., & Parasuraman, R. (2011). A meta-analysis of factors impacting trust in human-robot interaction. *Human Factors*, *53*, 517–527.

Hardin, R. (2006). *Trust*. Cambridge, UK: Polity.

Ho, G., Kiff, L. M., Plocher, T., & Haigh, K. Z. (2005). A model of trust and reliance of automation technology for older users. In *The AAAI 2005 Fall Symposium on Caring Machines* (pp. 45–50). Menlo Park, CA: AAAI Press.

Ho, G., Wheatley, D., & Scialfa, C. T. (2005). Age differences in trust and reliance of a medication management system. *Interacting With Computers*, *17*, 690–710.

Hoffman, R. R., Lee, J. D., Woods, D. D., Shadbolt, N., Miller, J., & Bradshaw, J. M. (2009). The dynamics of trust in cyberdomains. *IEEE Intelligent Systems*, *24*(6), 5–11.

Huerta, E., Glandon, T., & Petrides, Y. (2012). Framing, decision-aid systems, and culture: Exploring influences on fraud investigations. *International Journal of Accounting Information Systems*, *13*, 316–333.

Jamieson, G. A., Wang, L., & Neyedli, H. F. (2008). *Developing human-machine interfaces to support appropriate trust and reliance on automated combat identification systems*. Toronto, Canada: Department of National Defence.

Jian, J. Y., Bisantz, A. M., Drury, C. G, & Llinas, J. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*, 53–71.

Johnson, J. D. (2004). *Type of automation failure: The effects on trust and reliance in automation* (Master's thesis). Retrieved from ProQuest Dissertations and Theses.

Kaber, D. B., & Endsley, M. R. (2004). The effects of level of automation and adaptive automation on human performance, situation awareness and workload in a dynamic control task. *Theoretical Issues in Ergonomics Science*, *5*, 113–153.

Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces: Trustworthiness of cyber-banking system interfaces. *Interaction With Computers*, *10*, 1–29.

Koustanaï, A., Cavallo, V., Delhomme, P., & Mas, A. (2012). Simulator training with a forward collision warning system effects on driver-system interactions and driver trust. *Human Factors*, *54*, 709–721.

Lacson, F. C., Wiegmann, D. A., & Madhavan, P. (2005). Effects of attribute and goal framing on automation reliance and compliance. In *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting* (pp. 482–486). Santa Monica, CA: Human Factors and Ergonomics Society.

Lee, E.-J. (2008). Flattery may get computers somewhere, sometimes: The moderating role of output modality, computer gender, and user gender. *International Journal of Human-Computer Studies*, *66*, 789–800.

Lee, J. D., & Moray, N. (1992). Trust, control strategies and allocation of function in human machine systems. *Ergonomics*, *22*, 671–691.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, *46*, 50–80.

Lees, M. N., & Lee, J. D. (2007). The influence of distraction and driving context on driver response to imperfect collision warning systems. *Ergonomics*, *50*, 1264–1286.

Lerch, F. J., Prietula, M. J., & Kulik, C. T. (1997). The Turing effect: The nature of trust in expert system advice. In P. J. Feltovich, K. M. Ford, & R. R. Hoffman (Eds.), *Expertise in context: Human and machine* (pp. 417–448). Cambridge, MA: MIT Press.

Levinthal, B. R., & Wickens, C. D. (2006). Management of multiple UAVs with imperfect automation. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting* (pp. 1941–1944). Santa Monica, CA: Human Factors and Ergonomics Society.

Levs, J. (2012, January 15). What caused the cruise ship disaster? *CNN*. Retrieved from http://www.cnn.com/2012/01/15/world/europe/italy-cruise-questions/index.html

Li, D., Rau, P. P., & Li, Y. (2010). A cross-cultural study: Effect of robot appearance and task. *International Journal of Social Robotics*, *2*, 175–186.

Li, Y. M., & Yeh, Y. S. (2010, July). Increasing trust in mobile commerce through design aesthetics. *Computers in Human Behavior*, *26*, 673–684.

Lyons, J. B., & Stokes, C. K. (2012, February). Human–human reliance in the context of automation. *Human Factors*, *54*, 112–121.

Madhavan, P., & Phillips, R. R. (2010). Effects of computer self-efficacy and system reliability on user interaction with decision support systems. *Computers in Human Behavior*, *26*, 199–204.

Madhavan, P., & Wiegmann, D. A. (2005a). Cognitive anchoring on self-generated decisions reduces operator reliance on automated diagnostic aids. *Human Factors*, *47*, 332–341.

Madhavan, P., & Wiegmann, D. A. (2005b). Effects of information source, pedigree, and reliability on operators' utilization of diagnostic advice. In *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting* (pp. 487–491). Santa Monica, CA: Human Factors and Ergonomics Society.

Madhavan, P., & Wiegmann, D. A. (2007a). Effects of information source, pedigree, and reliability on operator interaction with decision support systems. *Human Factors*, *49*, 773–785.

Madhavan, P., & Wiegmann, D. A. (2007b). Similarities and differences between human-human and human-automation trust: An integrative review. *Theoretical Issues in Ergonomics Science*, *8*, 277–301.

Madhavan, P., Wiegmann, D. A., & Lacson, F. C. (2006). Automation failures on tasks easily performed by operators undermine trust in automated aids. *Human Factors*, *48*, 241–256.

Manzey, D., Bahner, J. E., & Hueper, A. D. (2006). Misuse of automated aids in process control: Complacency, automation bias and possible training interventions. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*

(pp. 220–224). Santa Monica, CA: Human Factors and Ergonomics Society.

Manzey, D., Reichenbach, J., & Onnasch, L. (2012). Human performance consequences of automated decision aids: The impact of degree of automation and system experience. *Journal of Cognitive Engineering and Decision Making*, *6*, 57–87.

Marsh, S., & Dibben, M. R. (2003). The role of trust in information science and technology. *Annual Review of Information Science and Technology*, *37*, 465–498.

Masalonis, A. J. (2003). Effects of training operators on situation-specific automation reliability. *IEEE International Conference on Systems, Man and Cybernetics*, 2, 1595–1599.

Mayer, A. (2008). *The manipulation of user expectancies: Effects on reliance, compliance, and trust using an automated system* (Unpublished master's thesis). Georgia Institute of Technology, Atlanta.

Mayer, A. K., Sanchez, J., Fisk, A. D., & Rogers, W. A. (2006). Don't let me down: The role of operator expectations in human-automation interaction. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting* (pp. 2345–2349). Santa Monica, CA: Human Factors and Ergonomics Society.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*, 709–734.

McBride, M., Carter, L., & Ntuen, C. (2012). The impact of personality on nurses' bias towards automated decision aid acceptance. *International Journal of Information Systems and Change Management*, *6*, 132–146.

McBride, S. E., Rogers, W. A., & Fisk, A. D. (2010). Do younger and older adults differentially depend on an automated system? *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting* (pp. 175–179). Santa Monica, CA: Human Factors and Ergonomics Society.

McBride, S. E., Rogers, W. A., & Fisk, A. D. (2011). Understanding the effect of workload on automation use for younger and older adults. *Human Factors*, *53*, 672–686.

McCarley, J. S., Wiegmann, D. A., Wickens, C. D., & Kramer, A. F. (2003). Effects of age on utilization and perceived reliability of an automated decision-making aid for luggage screening. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 340–343). Santa Monica, CA: Human Factors and Ergonomics Society.

McGarry, K. A. (2007). *Effects of false alarms and misses on reliance, compliance, and attention when using an automated warning system* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.

McGuirl, J. M., & Sarter, N. B. (2006). Supporting trust calibration and the effective use of decision aids by presenting dynamic system confidence information. *Human Factors*, *48*, 656–665.

Merritt, S. M. (2011). Affective processes in human-automation interactions. *Human Factors*, *53*, 356–370.

Merritt, S. M., Heimbaugh, H., LaChapell, J., & Lee, D. (2012). I trust it, but I don't know why: Effects of implicit attitudes toward automation on trust in an automated system. *Human Factors*, *55*, 520–534.

Merritt, S. M., & Ilgen, D. R. (2008). Not all trust is created equal: Dispositional and history-based trust in human–automation interaction. *Human Factors*, *50*, 194–210.

Nass, C., Moon, Y., & Carney, P. (1999). Are people polite to computers? Responses to computer-based interviewing systems. *Journal of Applied Social Psychology*, *29*, 1093–1109.

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computers are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 72–78). New York, NY: ACM.

Naef, M., Fehr, E., Fischbacher, U., Schupp, J., & Wagner, G. (2008). *Decomposing trust: Exploring national and ethnical trust difference*. Working Paper, Institute for Empirical Research in Economics, University of Zurich.

Neyedli, H. F., Hollands, J. G., & Jamieson, G. A. (2011). Beyond identity: Incorporating system reliability information into an automated combat identification system. *Human Factors*, *53*, 338–355.

Nomura, T., Kanda, T., Suzuki, T., & Kato, K. (2008). Prediction of human behavior in human–robot interaction using psychological scales for anxiety and negative attitudes toward robots. *IEEE Transactions on Robotics*, *24*, 442–451.

Oduor, K. F., & Campbell, C. S. (2007). Deciding when to trust automation in a policy-based city management game: Policity. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (p. 2). New York, NY: ACM.

Oduor, K. F., & Wiebe, E. N. (2008). The effects of automated decision algorithm modality and transparency on reported trust and task performance. In *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting* (pp. 302–306). Santa Monica, CA: Human Factors and Ergonomics Society.

Ou, C. X., & Sia, C. L. (2010). Consumer trust and distrust: An issue of website design. *International Journal of Human-Computer Studies*, *68*, 913–934.

Pak, R., Fink, N., Price, M., Bass, B., & Sturre, L. (2012). Decision support aids with anthropomorphic characteristics influence trust and performance in younger and older adults. *Ergonomics*, *55*, 1059–1072.

Parasuraman, R., & Miller, C. A. (2004). Trust and etiquette in high-criticality automated systems. *Communications of the ACM*, *47*(4), 51–55.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, *39*, 230–253.

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

Parkes, A. (2009, July). Persuasive decision support: Improving reliance on decision support systems. *Pacific Asia Journal of the Association for Information Systems*, *4*(3), 1–13.

Perkins, L., Miller, J. E., Hashemi, A., & Burns, G. (2010). Designing for human-centered systems: Situational risk as a factor of trust in automation. In *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting* (pp. 2130–2134). Santa Monica, CA: Human Factors and Ergonomics Society.

Phillips, R. R., & Madhavan, P. (2011). The effect of distractor modality and processing code on human-automation interaction. *Cognition, Technology & Work*, *13*, 233–244.

Pruitt, D. G., & Rubin, Z., (1986). *Social conflict: Escalation, statement, and settlement*. New York, NY: Random House.

Rajaonah, B., Tricot, N., Anceaux, F., & Millot, P. (2008). The role of intervening variables in driver–ACC cooperation. *International Journal of Human-Computer Studies*, *66*, 185–197.

Rau, P. L., Li, Y., & Li, D. (2009). Effects of communication style and culture on ability to accept recommendations from robots. *Computers in Human Behavior*, *25*, 587–595.

Reichenbach, J., Onnasch, L., & Manzey, D. (2011). Human performance consequences of automated decision aids in states of sleep loss. *Human Factors*, *53*, 717–728.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*, 95–112.

Rice, S. (2009). Examining single and multiple process theories of trust in automation. *Journal of General Psychology*, *136*, 303–322.

Rice, S., & Keller, D. (2009). Automation reliance under time pressure. *International Journal of Cognitive Technology*, *14*(1).

Rice, S., Trafimow, D., Clayton, K., & Hunt, G. (2008). Impact of the contrast effect on trust ratings and behavior with automated systems. *Cognitive Technology Journal*, *13*(2), 30–41.

Riedl, R., Hubert, M., & Kenning, P. (2010). Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. *MIS Quarterly*, *34*, 397–428.

Riedl, R., & Javor, A. (2012). The biology of trust. *Journal of Neuroscience, Psychology, and Economics*, *5*(2), 63–91.

Riley, V. (1996). Operator reliance on automation: Theory and data. *Automation and Human Performance: Theory and Application*, 1, 22–27.

Ross, J. M. (2008). *Moderators of trust and reliance across multiple decision aids* (Doctoral dissertation). University of Central Florida, Orlando.

Ross, J. M., Szalma, J. L., Hancock, P. A., Barnett, J. S., & Taylor, G. (2008). The effect of automation reliability on user automation trust and reliance in a search-and-rescue scenario. In *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting* (pp. 1340–1344). Santa Monica, CA: Human Factors and Ergonomics Society.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*, 651–665.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, *35*, 1–7.

Rovira, E., McGarry, K., & Parasuraman, R. (2007). Effects of imperfect automation on decision making in a simulated command and control task. *Human Factors*, *49*, 76–87.

Rovira, E., & Parasuraman, R. (2010). Transitioning to future air traffic management: Effects of imperfect automation on controller attention and performance. *Human Factors*, *52*, 411–425.

Sanchez, J. (2006). *Factors that affect trust and reliance on an automated aid* (Unpublished doctoral dissertation). Georgia Institute of Technology, Atlanta.

Sanchez, J., Fisk, A. D., & Rogers, W. A. (2004). Reliability and age-related effects on trust and reliance of a decision support aid. In *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting* (pp. 586–589). Santa Monica, CA: Human Factors and Ergonomics Society.

Sanchez, J., Rogers, W. A., Fisk, A. D., & Rovira, E. (2011). Understanding reliance on automation: Effects of error type, error distribution, age and experience. *Theoretical Issues in Ergonomics Science*. doi:10.1080/1463922X.2011.611269.

Sauer, J., Felsing, T., Franke, H., & Rüttinger, B. (2006). Cognitive diversity and team performance in a complex multiple task environment. *Ergonomics*, *49*, 934–954.

Schwark, J., Dolgov, I., Graves, W., & Hor, D. (2010). The influence of perceived task difficulty and importance on automation use. In *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting* (pp. 1503–1507). Santa Monica, CA: Human Factors and Ergonomics Society.

Seong, Y., & Bisantz, A. M. (2008). The impact of cognitive feedback on judgment performance and trust with decision aids. *International Journal of Industrial Ergonomics*, *38*, 608–625.

Seppelt, B. D., & Lee, J. D. (2007). Making adaptive cruise control (ACC) limits visible. *International Journal of Human-Computer Studies*, *65*, 192–205.

Spain, R. D. (2009). *The effects of automation expertise, system confidence, and image quality on trust, compliance, and performance* (Doctoral dissertation). Old Dominion University, Norfolk, VA.

Spain, R. D., & Madhavan, P. (2009). The role of automation etiquette and pedigree in trust and dependence. In *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting* (pp. 339–343). Santa Monica, CA: Human Factors and Ergonomics Society.

Stanton, N. S., Ragsdale, S. A., & Bustamante, E. A. (2009). The effects of system technology and probability type on trust, compliance, and reliance. In *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting* (pp. 1368–1372). Santa Monica, CA: Human Factors and Ergonomics Society.

Steinke, F., Fritsch, T., & Silbermann, L. (2012). A systematic review of trust in automation and assistance systems for older persons' overall requirements. In *eTELEMED 2012, the Fourth International Conference on eHealth, Telemedicine, and Social Medicine* (pp. 155–163). Valencia, Spain: IARIA.

Stokes, C. K., Lyons, J. B., Littlejohn, K., Natarian, J., Case, E., & Speranza, N. (2010). Accounting for the human in cyberspace: Effects of mood on trust in automation. In *Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems* (pp. 180–187). Chicago, IL: IEEE. doi:10.1109/CTS.2010.5478512

Szalma, J. L., & Taylor, G. S. (2011). Individual differences in response to automation: The five factor model of personality. *Journal of Experimental Psychology: Applied*, *17*(2), 71–96.

Thropp, J. E. (2006). *Individual preferences using automation* (Unpublished doctoral dissertation). University of Central Florida, Orlando.

Tung, F.-W. (2011). Influence of gender and age on the attitudes of children towards humanoid robots. In J. A. Jacko (Ed.), *Human-computer interaction, Part IV* (pp. 637–646). Berlin, Germany: Springer-Verlag.

Verberne, F. M., Ham, J., & Midden, C. J. (2012). Trust in smart systems sharing driving goals and giving information to increase trustworthiness and acceptability of smart systems in cars. *Human Factors*, *54*, 799–810.

Wakefield, R. L., Stocks, M. H., & Wilder, W. M. (2004). The role of web site characteristics in initial trust formation. *Journal of Computer Information Systems*, *45*, 94–103.

Wang, L., Jamieson, G. A., & Hollands, J. G. (2009). Trust and reliance on an automated combat identification system: The role of aid reliability and reliability disclosure. *Human Factors*, *51*, 281–291.

Wang, L., Jamieson, G. A., & Hollands, J. G. (2011, September). The effects of design features on users' trust in and reliance on a combat identification system. In *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting* (pp. 375–379). Santa Monica, CA: Human Factors and Ergonomics Society.

Weinstock, A., Oron-Gilad, T., & Parmet, Y. (2012). The effect of system aesthetics on trust, cooperation, satisfaction and annoyance in an imperfect automated system. *Work: A Journal of Prevention, Assessment and Rehabilitation*, *41*, 258–265. doi:10.3233/WOR-2012-0166-258.

Wetzel, J. M. (2005). *Driver trust, annoyance, and compliance for an automated calendar system* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses.

Wilkison, B. D. (2008). *Effects of mental model quality on collaborative system performance* (Master's thesis). Retrieved from ProQuest Dissertations and Theses.

Willems, B., & Heiney, M. (2002). *Decision support automation research in the en route air traffic control environment* (DOT/FAA/CT-TN02/10). Atlantic City International Airport, NJ: Federal Aviation Administration William J. Hughes Technical Center.

Willis, J., & Todorov, A. (2006). First impressions: Making up your mind after a 100-ms exposure to a face. *Psychological Science*, *17*, 592–598.

Workman, M. (2005). Expert decision support system use, disuse, and misuse: A study using the theory of planned behavior. *Computers in Human Behavior*, *21*, 211–231.

Yuviler-Gavish, N., & Gopher, D. (2011). Effect of descriptive information and experience on automation reliance. *Human Factors*, *53*, 230–244.

Zhou, T. (2011). The effect of initial trust on user adoption of mobile payment. *Information Development*, *27*, 290–300.

Kevin Anthony Hoff is a research assistant at the Information Trust Institute at the University of Illinois at Urbana-Champaign. He received a bachelor of science from the University of Illinois at Urbana-Champaign in 2012.

Masooda Bashir is an assistant professor at the Graduate School of Library and Information Science at the University of Illinois at Urbana-Champaign. She also has appointments at the Coordinated Science laboratory and directs social science research at the College of Engineering. Her areas of research interests lie at the interface of information technology, psychology, and society, especially how privacy, trust, and security factors intersect from a psychological point of view with information technology.

Date received: December 20, 2013
Date accepted: July 15, 2014