Novel Developments in Formal Methods for Human Factors Engineering

Matthew L. Bolton
University at Buffalo, the State University of New York

Formal methods are robust tools and techniques for modeling, specifying, and mathematically proving properties about (verifying) systems. They are particularly good at both finding unexpected problems that arise from complex system interactions and proving that specific types of problems will never manifest. Formal methods have predominantly been used in the analysis and design of computer hardware and software systems. However, a growing research area within the human factors engineering community has been examining how formal methods can be used to prove whether problems exist in systems that rely on human-automation and human-human interaction for their safe operation. This symposium contains four papers by researchers who have been pushing the boundaries of where and how formal methods can be used in human factors engineering.

INTRODUCTION

Formal methods are well-defined mathematical languages, tools, and techniques for the specification, modeling, and verification of systems (Wing, 1990). Specification properties are formulated to rigorously describe desirable system properties, systems are modeled using mathematical languages, and verification mathematically proves whether or not the model satisfies the specification. There are a number of different ways formal methods can be applied in practice. Early efforts were concerned with proving whether computer programs satisfied specifications by hand. In modern times, semi-automated interactive theorem proving tools have been developed to assist analysts in such evaluations (Bertot, Castéran, Huet, & Paulin-Mohring, 2004; Kaufmann, Moore, & Manolios, 2000; Shankar, Owre, Rushby, & Stringer-Calvert, 1999). However, even these tools require extremely skilled operators and extensive time to be used on large systems.

Approaches like model checking have been developed to make formal verification a fully automated process (Clarke, Grumberg, & Peled, 1999). In model checking, a formal model describes a system as a set of variables and transitions between variable values (states). Specifications are usually represented in temporal logic (Emerson, 1990). They assert properties about the temporal relationships between system elements using system model variables. Ultimately, verification is performed by exhaustively searching through the system model (often using an extremely efficient, abstracted representation of the model's statespace) to determine if specifications hold.

Formal methods have been predominantly used in the design and analysis of computer hardware and software systems. However, because they are extremely good at finding unexpected problems with interactions between components in complex environments, a growing body of research has been investigating how formal methods (and especially model checking) can be used in human factors engineering (Bolton, Bass, & Siminiceanu, 2013; Weyers, Bowen, Dix, & Palanque, 2017) to find problems in human-automation and human-human interaction. These works have predominantly focused on analyzing the usability of human-machine and human-computer interfaces (Abowd, Wang, & Monk, 1995; Campos & Harrison, 2008; Paternò, 1997); finding potential mode confusions and automation surprises (Bredereke & Lankenau, 2002; Campos & Harrison, 2011; Degani, 2004; Degani & Heymann, 2002; Joshi, Miller, & Heimdahl, 2003; Rushby, 2002); assessing the impact of normative human task behavior on system safety (Aït-Ameur & Baron, 2006; Bolton, Siminiceanu, & Bass, 2011; Houser, Ma, Feigh, & Bolton, 2015; Paternò & Santoro, 2001); assessing the impact of human errors included (Bastide & Basnyat, 2007; Fields, 2001) or generated (Bolton, 2015; Bolton & Bass, 2013; Bolton, Bass, & Siminiceanu, 2012; Pan & Bolton, 2016) in task analytic behavior models; or having problems arise organically from cognitive or perceptual models (Cerone, Lindsay, & Connelly, 2005; Curzon, Rukšėnas, & Blandford, 2007; Hasanain, Boyd, & Bolton, 2015; Hasanain, Boyd, Edworthy, & Bolton, 2017; Rukšėnas, Curzon, Back, & Blandford, 2007).

As new formal methods have emerged, researchers have been developing novel ways that formal methods can be used to enforce rigor in the design, evaluation, and analysis of human-interactive systems. This symposium showcases four papers that report cutting edge work in this area.

Below we provide an overview of each of these papers.

FORMAL REPRESENTATIONS OF HUMAN WORK FOR SIMULATION AND GRAPH ANALYSES

While formal modeling has been explored extensively for interfaces, task models, and cognitive architecture, there have been few formal models designed to represent the structure of human work. This is particularly important for exploring different concepts of operation and allocations of functions between humans and automated agents. Our first paper (Ma & Feigh, 2017) describes a formalism for capturing the concepts contained in Work Models that Compute (WMC) simulation models (Pritchett, Feigh, Kim, & Kannan, 2014). In particular, this paper describes an automated method for generating formal models from WMC simulations and illustrates this process with an air traffic application. The paper then shows how this formal abstraction can be used to improve workflows for developing simulation models, validate simulation concepts, and enable insights into the human factors of the system through the generation and analysis of graph structure.

PREDICTING UNEXPECTED HUMAN INTERACTIONS WITH AFFORDANCE-BASED AUTOMATA

Affordances are concepts from ecological psychology that describe the possible actions allowed by an object in the environment (Gibson, 1979). Because humans will ultimately perform the actions afforded by a system, understanding the system's affordances is extremely important for predicting how the system will be used. Despite their importance in the design of human-interactive systems and the potential problems unexpected human actions can cause, formal methods have never accounted for affordances. Our second paper (Abbate & Bass, 2017) introduces a formal modeling and verification approach that uses affordances to predict how humans will interact with a system. To accomplish this, the authors adapt a preexisting psychological formalism for use in formal verification analyses. In their approach, a formal model encompasses the objects in the environment, their spatial relationships, and the motor capabilities of the human. The authors use their approach to identify potentially unanticipated, problematic human interactions with a door in an aircraft cockpit.

A FORMAL METHODS APPROACH TO HUMAN RELIABILITY ANALYSIS

As discussed in the introduction, formal methods have been used to discover when and how human error can contribute to system failure and prove properties about the reliability of human-interactive systems. However, they have never been explicitly used for human reliability analyses, where the idea is to quantify (probabilistically) how likely erroneous human behaviors are. Probabilistic model checking extends model checking by allowing state transitions to have probabilities and specifications to be asserted using probabilistic temporal logic (Forejt, Kwiatkowska, Norman, & Parker, 2011; Kwiatkowska, Norman, & Parker, 2007). This enables analysts to both account for probabilistic behavior in their models and prove properties about the probabilities of system behaviors. Probabilistic model checking has been used in verifications that account for probabilistic, variable human behavior (Beckert & Wagner, 2009; Feng, Wiltsche, Humphrey, & Topcu, 2016; Rungta et al., 2013; Sadigh et al., 2014). However, probabilistic model checking has not been in human reliability analyses. Our third paper (Zheng, Bolton, Daly, & Feng, 2017) fills this gap by adapting human reliability analysis using the Cognitive Reliability Error Analysis Method (CREAM) (Hollnagel, 1998) for use with the Prism probabilistic model checker (Forejt et al., 2011; Kwiatkowska et al., 2007). The authors illustrate their novel approach with a community pharmacy dispensing application.

FORMAL METHODS FOR PREDICTING HUMAN INTENT

In teleoperations, humans and robot automation will often share control so that they can work together to accomplish system goals (Dragan & Srinivasa, 2013). In this situation, it can be beneficial for the robot to anticipate what the human will want to do to ensure safe and efficient operation. This becomes a particularly difficult problem when significant amounts of latency exist in the system. Our third paper (Cubuktepe & Topcu, 2017) addresses this problem with a data-driven approach to intent inference in shared control that can provide stochastic, formal guarantees about performance while accounting for this latency. Two case studies are used to demonstrate the capabilities of this method.

REFERENCES

Abbate, A. J., & Bass, E. J. (2017). Modeling affordance using formal methods. In *Proceedings of the International Annual Meeting of the Human Factors and Ergonomics Society.* Santa Monica: HFES.

Abowd, G. D., Wang, H., & Monk, A. F. (1995). A formal technique for automated dialogue development. In *Proceedings of the 1st Conference on Designing Interactive Systems* (pp. 219–226). New York: ACM.

Aït-Ameur, Y., & Baron, M. (2006). Formal and experimental validation approaches in HCI systems design based on a shared event B model. *International Journal on Software Tools for Technology Transfer*, *8*(6), 547–563.

Bastide, R., & Basnyat, S. (2007). Error patterns: Systematic investigation of deviations in task models. In *Task models and diagrams for users interface design* (pp. 109–121). Berlin: Springer.

Beckert, B., & Wagner, M. (2009). Probabilistic models for the verification of human-computer interaction. In *Annual conference on artificial intelligence* (pp. 687–694). Berlin.

Bertot, Y., Castéran, P., Huet, G. i., & Paulin-Mohring, C. (2004). *Interactive theorem proving and program development : Coq'art : the calculus of inductive constructions*. Berlin, New York: Springer.

Bolton, M. L. (2015). Model checking human–human communication protocols using task models and miscommunication generation. *Journal of Aerospace Information Systems*, *12*(7), 476–489.

Bolton, M. L., & Bass, E. J. (2013). Generating erroneous human behavior from strategic knowledge in task models and evaluating its impact on system safety with model checking. *IEEE Transactions on Systems, Man and Cybernetics: Systems*, *43*(6), 1314–1327.

Bolton, M. L., Bass, E. J., & Siminiceanu, R. I. (2012). Generating phenotypical erroneous human behavior to evaluate human-automation interaction using model checking. *International Journal of Human-Computer Studies*, *70*(11), 888–906.

Bolton, M. L., Bass, E. J., & Siminiceanu, R. I. (2013). Using formal verification to evaluate human-automation interaction in safety critical systems, a review. *IEEE Transactions on Systems, Man and Cybernetics: Systems*, *43*(3), 488–503.

Bolton, M. L., Siminiceanu, R. I., & Bass, E. J. (2011). A systematic approach to model checking human-automation interaction using task-analytic models. *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, *41*(5), 961–976.

Bredereke, J., & Lankenau, A. (2002). A rigorous view of mode confusion. In *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security* (pp. 19–31). London, UK: Springer.

Campos, J. C., & Harrison, M. D. (2008). Systematic analysis of control panel interfaces using formal tools. In *Proceedings of the 15th International Workshop on the Design, Verification and Specification of Interactive Systems* (pp. 72–85). Berlin: Springer.

Campos, J. C., & Harrison, M. D. (2011). Modelling and analysing the interactive behaviour of an infusion pump. In *Proceedings of the Fourth International Workshop on Formal Methods for Interactive Systems.* Potsdam: EASST.

Cerone, A., Lindsay, P. A., & Connelly, S. (2005). Formal analysis of human-computer interaction using model-checking. In *Proceedings of the 3rd IEEE International Conference on Software Engineering and Formal Methods* (pp. 352–362). Los Alamitos: IEEE Computer Society.

Clarke, E. M., Grumberg, O., & Peled, D. A. (1999). *Model checking*. Cambridge: MIT Press.

Cubuktepe, L., & Topcu, U. (2017). Intent prediction in shared control with delayed feedback. In *Proceedings of the International Annual Meeting of the Human Factors and Ergonomics Society.* Santa Monica: HFES.

Curzon, P., Rukšėnas, R., & Blandford, A. (2007). An approach to formal verification of humanÚcomputer interaction. *Formal Aspects of Computing*, *19*(4), 513–550.

Degani, A. (2004). *Taming HAL: Designing interfaces beyond 2001*. New York: Macmillan.

Degani, A., & Heymann, M. (2002). Formal verification of human-automation interaction. *Human Factors*, *44*(1), 28–43.

Dragan, A. D., & Srinivasa, S. S. (2013). A policy-blending formalism for shared control. *The International Journal of Robotics Research*, *32*(7), 790–805.

Emerson, E. A. (1990). Temporal and modal logic. In J. van Leeuwen, A. R. Meyer, M. Nivat, M. Paterson, & D. Perrin (Eds.), *Handbook of theoretical computer science* (pp. 995–1072). Cambridge: MIT Press.

Feng, L., Wiltsche, C., Humphrey, L., & Topcu, U. (2016). Synthesis of human-in-the-loop control protocols for autonomous systems. *IEEE Transactions on Automation Science and Engineering*, *13*(2), 450–462.

Fields, R. E. (2001). *Analysis of erroneous actions in the design of critical systems* (Unpublished doctoral dissertation). University of York, York.

Forejt, V., Kwiatkowska, M., Norman, G., & Parker, D. (2011). Automated verification techniques for probabilistic systems. In M. Bernardo & V. Issarny (Eds.), *Formal methods for eternal networked software systems (sfm'11)* (Vol. 6659, pp. 53–113). Berlin: Springer.

Gibson, J. J. (1979). *The ecological approach to visual perception*. Boston: Houghton Mifflin.

Hasanain, B., Boyd, A., & Bolton, M. (2015). Using model checking to detect simultaneous masking in medical alarms. *IEEE Transactions on Human-Machine Systems*, *46*, 174–185.

Hasanain, B., Boyd, A. D., Edworthy, J., & Bolton, M. L. (2017). A formal approach to discovering simultaneous additive masking between auditory medical alarms. *Applied Ergonomics*, *58*, 500 - 514.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*. Oxford: Elsevier.

Houser, A., Ma, L. M., Feigh, K., & Bolton, M. L. (2015). A formal approach to modeling and analyzing human taskload in simulated air traffic scenarios. In *Proceedings of the ieee 2015 international conference on complex systems engineering* (pp. 1–6). Piscataway: IEEE.

Joshi, A., Miller, S. P., & Heimdahl, M. P. (2003, October). Mode confusion analysis of a flight guidance system using formal methods. In *Proceedings of the 22nd Digital Avionics Systems Conference* (pp. 2.D.11–2.D.112). Piscataway: IEEE.

Kaufmann, M., Moore, J. S., & Manolios, P. (2000). *Computer-aided reasoning: An approach*. Norwell, MA, USA: Kluwer Academic Publishers.

Kwiatkowska, M., Norman, G., & Parker, D. (2007). Stochastic model checking. In M. Bernardo & J. Hillston (Eds.), *Formal methods for the design of computer, communication and software systems: Performance evaluation* (Vol. 4486, pp. 220–270). Berlin: Springer.

Ma, L. M., & Feigh, K. (2017). Jumpstarting modelling systems design: A generalized xml abstraction of simulation models. In *Proceedings of the International Annual Meeting of the Human Factors and Ergonomics Society.* Santa Monica: HFES.

Pan, D., & Bolton, M. L. (2016). Properties for formally assessing the performance level of human-human collaborative procedures with miscommunications and erroneous human behavior. *International Journal of Industrial Ergonomics*.

Paternò, F. (1997). Formal reasoning about dialogue properties with automatic support. *Interacting with Computers*, *9*(2), 173–196.

Paternò, F., & Santoro, C. (2001). Integrating model checking and HCI tools to help designers verify user interface properties. In *Proceedings of the 7th International Workshop on the Design, Specification, and Verification of Interactive Systems* (pp. 135–150). Berlin: Springer.

Pritchett, A. R., Feigh, K. M., Kim, S. Y., & Kannan, S. K. (2014). Work models that compute to describe multiagent concepts of operation: Part 1. *Journal of Aerospace Information Systems*, *11*(10), 610–622.

Rukšėnas, R., Curzon, P., Back, J., & Blandford, A. (2007). Formal modelling of cognitive interpretation. In *Proceedings of the 13th International Workshop on the Design, Specification, and Verification of Interactive Systems* (pp. 123–136). London: Springer.

Rungta, N., Brat, G., Clancey, W. J., Linde, C., Raimondi, F., Seah, C., & Shafto, M. (2013). Aviation safety: Modeling and analyzing complex interactions between humans and automated systems. In *Proceedings of the 3rd international conference on application and theory of automation in command and control systems* (pp. 27–37). New York: ACM.

Rushby, J. (2002). Using model checking to help discover mode confusions and other automation surprises. *Reliability Engineering and System Safety*, *75*(2), 167–177.

Sadigh, D., Driggs-Campbell, K., Puggelli, A., Li, W., Shia, V., Bajcsy, R., ... Seshia, S. A. (2014). Data-driven probabilistic modeling and verification of human driver behavior. In *Proceedings of the aaai spring symposium on formal verification and modeling in human-machine systems.* Palo Alto: AAAI.

Shankar, N., Owre, S., Rushby, J. M., & Stringer-Calvert, D. W. J. (1999, September). Pvs prover guide [Computer software manual]. Menlo Park, CA.

Weyers, B., Bowen, J., Dix, A., & Palanque, P. (Eds.). (2017). *The handbook of formal methods in human-computer interaction*. Berlin: Springer.

Wing, J. M. (1990). A specifier's introduction to formal methods. *Computer*, *23*(9), 8, 10–22, 24.

Zheng, X., Bolton, M. L., Daly, C., & Feng, L. (2017). A formal human reliability analysis of a community pharmacy dispensing procedure. In *Proceedings of the International Annual Meeting of the Human Factors and Ergonomics Society.* Santa Monica: HFES.