Why IT systems for emergency response get rejected: examining responders' attitude to IT

Erion Elmasllari
User-Centered Ubiquitous Computing
Fraunhofer FIT
Schloss Birlinghoven
53754 Sankt Augustin, Germany
erion@elmasllari.com

ABSTRACT

Emergency responders' attitude to IT is marked by resistance, aversity, and rejection. This attitude is specific to IT alone and does not extend to technology in general. Current research on the topic only presents partial, scattered, and unconnected accounts that do not provide a starting point on how to tackle the rejection. The available models for technology acceptance are also too general and do not take into account the specifics of the emergency response domain.

Through extensive user research combined with a grounded theory approach, this paper identifies twelve problem areas from which responders' negative attitude towards IT arises. By extending the technology acceptance models with this new knowledge, we provide system designers with an understanding of what to tackle and tune in their IT system designs so that a positive attitude among emergency responders can be achieved.

Keywords

Acceptance of ICT, Survey on existing approaches, Impact of IT, Grounded Theory

INTRODUCTION

Multiple studies[1] have reported that emergency responders' attitude to IT is one of resistance, if not outright rejection. A firefighter summarized the current situation as: "We have two proud centuries of tradition unhampered by progress"[2]. This attitude, however, cannot be dismissed as simple resistance to change. The same firefighter – just like many others in (BRIDGE 2011) – proudly told us how all processes and tools at his department had changed within his lifetime, with some of the changes even stemming from his own ideas. Among emergency responders, aversity to IT is only about IT, not about change or technology in general.

The attitude of responders to IT has been object of several research papers, but these have only provided partial glimpses, scattered and unconnected to each other. The research results, consisting mostly of observations and matter-of-fact evidence, have not been distilled into a clear set of core motives that drive the attitude. The present paper lifts these limitations:

1. It identifies the root causes and sheds light on the underlying issues of responders' attitude to IT.
2. It abstracts the evidence into a model of the multiple facets of this attitude.
3. It extends technology acceptance models in a way that can be directly used by system designers and project managers alike.

[1] To name just a few: Paul et al. 2008; Orthner et al. 2005; BRIDGE 2011; Adler et al. 2012; Ammenwerth et al. 2006b.
[2] Source: Personal interview with a Denver firefighter, May 2017.

STATE OF THE ART AND RESEARCH METHODOLOGY

Several technology acceptance models (Venkatesh et al. 2003; Dishaw et al. 2002; Ammenwerth et al. 2006b; Goodhue and Thompson 1995) link an individual's past experience with IT to their present attitude towards IT and to their future decision to use IT for a given task (see figure 1). While we do not dispute these models' validity, we note that none of the models consider the context, stress, and task overload that are typical of disaster and emergency response, even though stress is known to magnify negative feelings and attitudes (Seaward 2016).

Owing to their aim for general applicability, the technology acceptance models use very generic and abstract terms, which are difficult or impossible to relate with concrete aspects and concepts from the emergency response domain. As a result, it becomes impossible to know what aspects of IT give rise to which facets of the responders' attitude. This missing causality link leaves system designers powerless to either understand the problems or correct them.

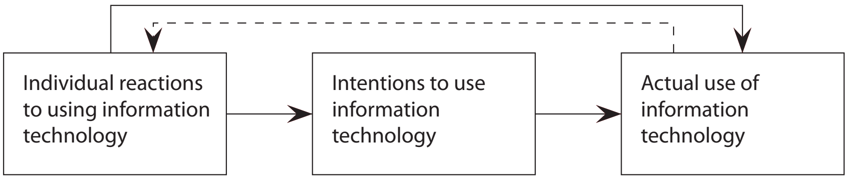

Figure 1. Commonalities of various technology acceptance models

As part of the DERMIS framework for emergency systems, (Turoff et al. 2004) name several concrete factors that impact the acceptance of IT among emergency responders. However, this is only done tangentially; DERMIS neither addresses, nor explains attitude to IT in emergency response front lines. The focus of the framework lies on *management* information systems for emergencies, a context where attitude to IT is traditionally positive (see section "Scope of the attitude to IT").

This paper is based on research carried out over four years in seven countries as part of the BRIDGE project[3], an EU-funded FP7 research whose goal is to develop technical and organizational solutions for inter-agency, cross-border crisis and emergency management. A combination of literature research, document analysis, and user-centered participatory design methods (Greenbaum 1991) were used to elicit and analyze the needs and problems of first responders with regard to ICT on the front lines. More than 300 hours of interviews, participant and non-participant observations, workshops, and other empiric research methods were carried out involving triagers, firefighters, paramedics, doctors, police, disaster relief workers, and incident commanders from Norway, UK, Netherlands, Ireland, Switzerland, Austria, and Germany[4]. At least two different methods of investigation were used for each question, as recommended by (Sanders 1992). An advisory board of responders accompanied the whole research in the role of a continuous focus group.

Due to the scarcity of pre-existing explanations and hypotheses for the responders' attitude to IT, a grounded theory approach (Glaser and Strauss 1967) was undertaken to group the findings and identify overarching patterns and issues. The coding and grouping of the gathered data identified twelve problem areas stemming from the introduction of IT. This is where the needs and practices of responders – especially in the front lines – clash with IT, giving rise to the reported aversity. The identified problem areas are discussed in detail in the next section.

SCOPE OF THE ATTITUDE TO IT

Technologists and decision makers commonly group Information Technology (IT) and Communication Technology (CT) under the same term: ICT[5]. First responders, however, see IT and CT as two very different things, for which different attitudes apply. While strongly resisting IT, responders use and trust CT in every facet of their work: radio on the front lines, phones, fax, and cellphones in higher levels of the response and where the infrastructure allows for it (Bhudhiraja 2015; Schmidt 2007).

[3] http://www.bridgeproject.eu/en

[4] In detail: THW Germany; Firefighters of Bonn (Germany), St. Gallen and Flums (Switzerland), Cork (Ireland), and Denver (US); Norwegian Air Ambulance and the Regional Centre for Emergency Medical Research and Development in Stavanger, Norway; Police representatives from Hertfordshire (UK) and Ghent (Belgium); the German Army at Ludwigshafen (Germany).

[5] For the remainder of this paper, we will use IT to refer to computers, software, middleware, storage, and input/output peripherals dedicated to information processing, and we will use CT to refer to radio, telephone, fax, voice, and other technologies whose primary goal is to enable people to communicate with each other. Technologies such as chat, VoIP, etc., fall under IT, because complex software stacks both play a crucial role and cannot be abstracted away, especially when failures occur. It is thus impossible to see the communication aspects of these technologies as separate from the underlying IT components.

Attitude towards IT strongly correlates with the position of a responder in the hierarchy and with the distance from the emergency scene (front- vs back-lines of response). Thus, the higher up the organizational hierarchy a responder is, and the farther away she is from front-line response, the higher the chances are that she uses and trusts IT systems in her daily work. Typical examples of IT at these levels include decision support systems, GIS databases, and other support systems. Responders at the higher levels of the hierarchy typically work in a well-established, predictable workflow, perform remote-command, managerial, or strategy roles, and use IT for disaster prevention tasks, strategy planning, and high-level or remote management (Bhudhiraja 2015). The nitty-gritty details and unpredictable situations on the ground turn here to simple statistics, record-keeping, or if-then decisions, which are all easily supported by IT. Consistent to this observation, (Paul et al. 2008) found out that EMS personnel have a negative and distrusting attitude towards IT, whereas for personnel from the emergency department at the hospital "...all the orders are on computers"[6]. As another example, (Orthner et al. 2005) report that hospital emergency departments commonly use computerized records, while first-line response agencies still use paper, voice, and fax.

Agent- and robot-based systems for gathering response-relevant data from the environment, from social networks, or other sources have been developed and deployed successfully, but hierarchy plays a role here as well. Citing (Sklar et al. 2014), "In any real-world deployment, a human will ultimately be responsible for the robot team's actions, typically a senior officer at tactical or strategic level"." Where UAVs and robot systems have been used successfully in the front lines, such as (Mohsin et al. 2016; Ramchurn et al. 2015), they function as an extension of the commander's senses, but they are not a tool that each front-line responder needs to grapple with.

SOURCES OF THE ATTITUDE TO IT

Current IT-based tools have a low cost-benefit ratio for first-line emergency response (Paul et al. 2008). Through extensive user and document research, we have identified the following crucial areas in which IT's drawbacks and cognitive costs give rise to the reported negative attitude.

Reliability

IT is not reliable enough for the needs of first responders, especially those in front-line emergency and disaster response. Even in less stressful environments, such as hospitals with a large and established IT infrastructure, physicians are reported to stop using IT and work on paper when they face many patients in a short time (Paul et al. 2008). The authors quote a physician as saying "...A situation like this is the time when the IT system gets overwhelmed". Firefighter commanders told us that they prefer to use whiteboards, flip-charts, and markers, because "they will not turn off as soon as power goes away, nor will they crash" (BRIDGE 2011). The availability of networking and IT infrastructure is another concern: "technology is good except when you are in the middle of the boondocks[7]" (Paul et al. 2008). IT for responders "must work. If I could rely on [the system], it would certainly be a relief" (Adler et al. 2012).

For agent-based systems, reliability means more than simply "not crashing". The agent's knowledge needs to be perceived as reliable too. Bellamy et al. 2017 report that "[agent-based systems] will be extraordinarily knowledgeable in very restricted domains — but this only exacerbates the problem of what happens when the user steps off the plateau of [the agent's] expertise [...] People are not accustomed to such discontinuities of competence."

Interoperability

Current IT-based tools are not easily interoperable with each other, nor can their parts be "mixed-and-matched" to repair a system or build a new one. There is often not even a common interoperability standard for IT-based emergency response tools. Federal countries, like Germany, the US, and Australia commonly have differing standards in neighboring states (Nocera and Garner 1999). Even when a country manages to choose a standard, its systems are typically not interoperable with the neighbor country. In comparison to IT, voice and paper have developed over thousands of years to be interoperable at a basic, subconscious level for humans. They can be used at any time, any place, and remain interoperable across borders or between different agencies. This is one of the keys to understanding why CT is so well-accepted: it simply extends the range of voice and paper over long distances, but does not restrict the message in any way. IT instead restricts the message contents, its formats, and the actions one can apply to that message.

[6]EMS personnel work on what can be seen as "the front lines" of an emergency call, while ED personnel work in a more controlled, less time-critical environment.

[7]Boondocks: a rural area (Merriam Webster 2017). Slang term referring to a place far from civilization.

Emergent behavior and improvisation

The ability to use a tool in an unforeseen role or context is essential for the emergency response domain. As a corollary, emergent behavior – behavior which was not designed on purpose – is expected from all the tools and systems[8]. IT systems for first-line emergency response typically do not support emergent behavior, they cannot be easily interfaced with each other, and they cannot be easily used to improvise. So far, IT has provided improvisation and emergent behavior only to the higher levels and the back-lines of emergency response. One could even argue that the best examples of this emergent behavior, such as Facebook's "I'm safe" notifications, the Ushahidi disaster maps, and the Twitter offers for "bed and breakfast for disaster victims"[9], arose from the public's IT tools, not from those of emergency responders.

Usability

Commercially available software is generally a hindrance in disaster response because of the limited functionality it offers (Paul et al. 2008). This is not a design fault as much as it is an inherent problem in the context. Even if software could support all the response situations and needs known up to the publication date, it still cannot adapt its behavior, data model, and functionality to match the needs of future, unknown disasters.

Worse than the limited functionality, commercial IT-based systems generally suffer from bad interface usability. This problem becomes critical in time-constrained and task-loaded situations, such as emergency response. Independently of how often they use computers in their daily work, both paramedics and emergency department personnel felt that "using current IT systems would constrain them in a disaster situation and they would prefer using paper to computers" (Paul et al. 2008).

In comparison to IT, where software interfaces are the norm, CT interfaces are often hardware-based. They have a long tradition and are based on well-known, long-lived standards and paradigms which incorporate usability lessons learned over decades. Software interfaces are, instead, much more varied and are based on comparatively short-lived paradigms[10]. Some of their lessons are not transferrable, whereas each new paradigm also introduces new kinds of usability problems.

Skill- and knowledge-based behavior

According to (Rasmussen 1983), human behavior can be skill-based (well-known, automatic, habitual, requiring no conscious thought), rule-based ("if X then do Y"), or knowledge-based (conscious mental processing, complex decisions for unfamiliar problems). The distinction between these three kinds of behavior is crucial for understanding responders' attitude to IT. Because every incident is different and unfamiliar, the responders' conscious mind is busy planning strategies and high-level actions. The responder's tools therefore *must* work at the skill- or rule-based levels of behavior. Unfortunately, current IT-based tools do not respect this:

1. They introduce changes into skill-based workflows, making them knowledge-driven. The responder's behavior becomes vulnerable to strong habit intrusion errors – performing the old, habitual workflow instead of the new one (Embrey 2003). Considerable training is then required to return these newly changed workflows to a skill-level behavior.
2. They often require the responders' explicit attention, e.g., to input data or to deal with a software problem. The behavior of responders then again becomes knowledge-driven.

In both cases, the drawback of knowledge-driven behavior is that it is very slow and highly error prone. In a situation where a mistake can cost a victim's or a responder's own life, it is easy to understand why responders are reluctant to accept IT, especially when it is mandated externally, and the more so when IT is not fully under the responder's control.

---

[8] All of the definitions of "emergent behavior" revolve around the idea that emergent behavior arises only when the system is put to use. Such behavior cannot be predicted at system design time and is not merely the sum of the individual behaviors of each single component of the system.

[9] When a disaster happens, people notify each other on Facebook that they are safe, mark on Google maps/Ushahidi places where help or resources are needed, and offer each other shelter on Twitter. All these behaviors were emergent; none of them was foreseen during the design of those social networks.

[10] As an example, the basic keypad design on the telephone has not changed in the last 70 years (Deininger 1960), whereas the Push-To-Talk interaction for radios has existed for the better part of a century. In comparison, at least five software interface paradigms, each with their own incompatible variations, have come and gone in the last 30 years of IT's life.

Impact on workflows and responsibilities

Like any complex system, an organization's formal rules – the ones the organization purports to follow – are always in a degraded state. They are never detailed enough, or, alternatively, they are so detailed that they contradict each other to a deadlock. It is only thanks to people's improvisation – their informal tasks – that the organization can work[11].

Introducing and adapting IT in an organization requires a fine alignment of the system to both the formal and the informal tasks (Ammenwerth et al. 2006a; Ammenwerth et al. 2006b), but this is oftentimes neglected. (Ritter et al. 2014) report that many medical systems are never used because they either introduce practices that conflict with other aspects of the user's job, or they require changes that affect other people's responsibilities. The same can be said about IT systems for emergency response: they often reshuffle tasks, workflows, and responsibilities in a way that does not match the organization's reality, or in a way that hinders some response steps to the benefit of others.

Oftentimes an organization has certain formal rules that are in reality never followed. IT systems cause such rules to be highlighted, because as soon as the rules are enforced by the system, it becomes clear how dysfunctional they are (Ammenwerth et al. 2006a). The organization then hurries to change, fix, or repeal these rules. At this point, the IT system becomes a hindrance and may get cast aside, because it continues to enforce the old, dysfunctional rule set. As an antidote to this problem, system designers should always very carefully analyze both the formal and the informal context in response organisations.

Some rescue-related processes require a certain preparation time (e.g., driving supplies to the incident area). Because other (slow) processes are carried out in parallel during this preparation time, there is rarely a large waiting gap and the workflow *seems* relatively smooth. When IT speeds up one of the processes, it risks disrupting the choreography of the response as a whole. (Büscher et al. 2016) report that in the Haiti earthquake, the agencies' search and rescue workflow was badly disrupted when the victims "made the process quicker" by using mobile phones to call for help, instead of waiting to be found.

The price of structured data

When writing things down on paper, the first responder uses it as an extension of her memory. The data is free-form, maybe structured in a way that makes sense to the responder, but this structure is developed on the spot, depends on the order in which events are witnessed, and is unique to the responder. Interoperability and compatibility with other responders is ensured by virtue of the data being expressed in a human language, most often in the responders' mother tongue. Interoperability and compatibility within the same profession is also supported by the practitioners' shared vocabulary.

In comparison, most IT approaches so far offer interfaces that support only structured data entry. These interfaces are not perceived as an extension to memory, but as an explicit data entry task. Citing (Paul et al. 2008): "EMS personnel find it difficult to use hand-held technology that constrains free-form data entry. [Whereas] CT enables the communication of unstructured information in the form of natural language, IT forces [responders] to convert [their] verbal communications into the schema of underlying databases". The authors also report that "EMS personnel do not carry computers on ambulances or helicopters; even when installed they will be used for communication, not for information". In our observations and user research we also noticed responders using a smartphone to send photos or recordings of the scene (i.e., communicate unstructured information). In essence, they were using IT to perform a CT task.

The adoption of IT for its primary purpose, information processing, is higher in remote command rooms, but paper has a stronghold here as well. As there is currently no seamless information flow between CT and IT, data coming through CT have to be entered into IT systems by a human. When users can't extract structured information from unstructured communication, or when they are overloaded with information, they revert to paper and verbal communication and simply drop IT (Paul et al. 2008).

Information-pull paradigm

Many work processes in disaster response are built around information that is saved directly on the world. To name a few examples: triagers mark victims visibly with a color to distinguish them, firefighters put knots on their lifelines to know which way the exit is, medics write important notes on the victims' face or body, and firefighter search troupes leave marks on doors to signify whether somebody is still inside (see figure 2). This information is

[11]Organizations are complex socio-technical systems and have the characteristics typical of this class of systems. One of the characteristics of such systems is that they are always degraded (Cook 1998).

pushed automatically from the world into the senses of other responders, just in time, as soon as they come to the place where they need this knowledge. To continue our examples: Paramedics see the triage color as soon as they come near the victim, firefighters can feel the knots whenever they follow the rope as a guide, and other medics can read the notes on a victim's face as soon as they start treating the victim. Current IT tools, instead, rarely push information to the responders who need it (Paul et al. 2008). The information available through such tools must be actively requested – pulled – by responders.

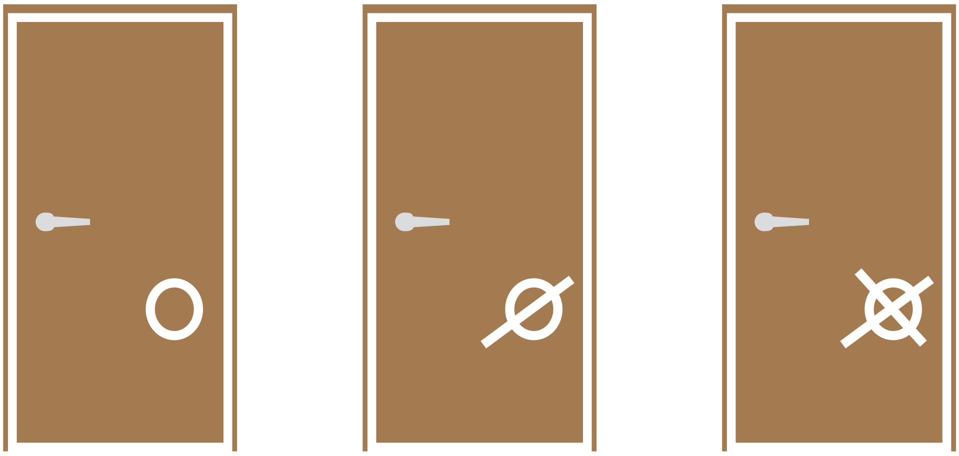

Figure 2. Search troupe chalk marks and their meaning.

Displacement of authority

Before the widespread use of CT, when there was no direct communication between involved parties, authority was correlated to hierarchy, e.g., only commanders could request additional resources or trigger certain response steps. CT allowed authority to flow downwards to the front-line responders, because they had the best view of the situation[12]. Now, with IT's automated workflows, required data fields, and automated decisions, (some) authority is again removed from front-line responders and relegated to the system. However, because the system's decisions arise deterministically from its software, the *real* decision authority lies not with the responders, not even with the system, but with the IT company who wrote the software. Authority is thus not only displaced geographically away from the front lines, but it is also displaced back in time, to when the design of the IT system was finalized.

Overturning of the key concepts of "truth" and "right"

The ability to log every action, decision, movement, and measurement, which is inherent in IT systems, opens the way to recording, reconstructing, and evaluating a responder's actions (Jentsch et al. 2013). However, the "truth" that is reconstructed from the logs will be incomplete and different from what actually happened, because there are no ways to record the conflicting informations, perceptions, experience, and thoughts that caused a responder to take a certain action or decision[13]. Under this new, "reconstructed" truth, actions that were right in the triager's frame of reference may suddenly appear wrong, leading to unjust blame and punishment. To complicate matters even further, this problem, which is introduced by IT, cannot be solved by IT alone. All possible solutions[14] involve re-educating organizations and societies to not seek blame. Excellent and concrete guidance on the matter can be found in (Dekker 2013).

Loss of flexibility

Traditional emergency response tools and workflows allow almost any element to be redefined, replaced, or left out on the spot. No triage tags? Use colored clothespins or spray paint on people's faces. No fax? Send someone to dispatch a message. Emergency responders are, in a sense, "hackers" and "programmers" of the response effort. They know how to "reprogram" and redefine response activities at will and on the fly. The introduction of IT

[12]Source: Personal interview with a Denver firefighter, May 2017. See also (Turoff et al. 2004).

[13]The responder typically cannot complete or correct this picture from memory, because her actions, being at the skill level, were automated and subconscious.

[14]Anonymizing data before evaluation, refraining from evaluating a responder's actions.

systems reduces this flexibility despite the designers' best intentions, because the IT system – especially its software – cannot be left out or replaced on the fly by the responders themselves. Flexibility is further diminished in another way as well. All current IT interaction paradigms hardcode what they expect from the user[15], making it impossible to redefine the system's actions without completely reprogramming the software.

Subjective perception

The acceptance of any tool or technology is influenced by the subjective perception of benefit: A person can't use or accept what she doesn't see as beneficial (Paul et al. 2008). On the other hand, people also can't see the benefits of something until they use it and get some positive experiences with it. Because all responders start their work at the front lines, with a CT and paper approach, and because most of them do not rise high enough in the hierarchy to a level where IT tools are widely used, they end up in a vicious circle. These responders never get a positive experience with IT at work, they get enough bad experiences with IT in real life or from hearsay, so they prejudice IT already before its introduction.

EXTENDING THE TECHNOLOGY ACCEPTANCE MODELS

In the discussion on state of the art, we pointed out that current technology acceptance models do not consider the particulars of the emergency response domain, or, alternatively, they are so general that the particulars of this domain are lost in the abstraction. Due to their generic terms, current technology acceptance models also do not give system designers any concrete starting point or problem that can be directly tackled to improve the design of systems for emergency response. Both of these shortcomings can be solved with the knowledge provided in the previous section. Thus, the problem areas and sources of attitude to IT represent concrete points for system designers to tackle. Furthermore, knowledge of these sources allows for extending technology acceptance models as in figure 3, preserving their qualities while at the same time grounding them to the emergency response domain.

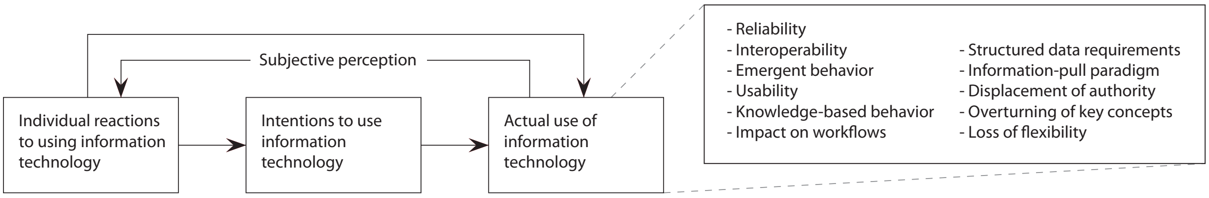

Figure 3. Extension of technology acceptance models for the emergency response domain

The revised model is based on the proposition that actual use of IT raises concerns in each of the discussed problem areas. These concerns then become the basis for (negative) individual reactions to IT, but cannot be balanced by positive use cases and reactions, because the hierarchy characteristics of IT in emergency response cause such positive examples to be present only in the higher and remote-command hierarchy levels. Subjective perception thus remains negative and in turn feeds back onto the responders' individual attitude towards IT, reinforcing the aversity.

CONCLUSION AND OUTLOOK

This paper presented the results of a detailed study which aimed at identifying the root causes of responders' negative attitude to IT in emergency response. Through extensive user research combined with a grounded theory approach, the issues expressed by responders were categorized into twelve problem areas from which the negative attitude towards IT arises. The paper thus solves the limitations of current research into the topic. It raises the state of the knowledge from reports and observations to a more general concept model that both explains the attitude and provides actionable points to improve it. Unlike current, generic IT acceptance models, the model we present is rooted in the emergency response domain and speaks the same language.

That said, this paper is only the beginning of a deeper investigation into the issue of acceptance of IT in emergency response front lines. Several questions remain open for future work:

- Are there other key concepts determining acceptance?

[15] Hardcoding is best clarified by an example. Consider the task of showing where response resources are located. In the implicit interaction paradigm, the system might be programmed to recognize drawings on a whiteboard and create a map automatically. In the explicit interaction paradigm, somebody would have to drag and drop icons on the screen. Now, imagine that instead of the whiteboard or screen, responders use Playmobil® figurines on a table. Every responder would immediately understand the new representation, but neither the implicit nor the explicit interaction paradigms would know what to do with it.

- Are the presented concepts and problem areas disjoint or do they depend on each other to some degree?
- Given that the research was carried out in the EU, how does the model apply to emergency response in other countries?
- What are some best practices to tackle each of the problem areas presented in the model?

ACKNOWLEDGEMENTS

This work was carried out under the EU FP7 BRIDGE Project, Grant No. 261817, and the EU Horizon 2020 MONICA Project, Grant No. 732350.

REFERENCES

Adler, T., Jakob, L., and Krüsmann, M. (2012). "Die Einführung neuer Technologien im Rettungsdienst - Akzeptanzforschung mit GABEK® dargestellt am Projekt e-Triage". In: *GABEK V: Werte in Organisationen und Gesellschaft*. Innsbruck u.a.: StudienVerlag, pp. 307–324.

Ammenwerth, E., Talmon, J., Ash, J., Bates, D., Beuscart-Zéphir, M., Duhamel, A., Elkin, P., Gardner, R., and Geissbuhler, A. (2006a). "Impact of CPOE on mortality rates - Contradictory findings, important messages". In: *Methods of Information in Medicine* 45.6, pp. 586–593.

Ammenwerth, E., Iller, C., and Mahler, C. (2006b). "IT-adoption and the interaction of task, technology and individuals: a fit framework and a case study". In: *BMC Medical Informatics and Decision Making* 6.1, pp. 1–13.

Bellamy, R. K. E., Andrist, S., Bickmore, T., Churchill, E. F., and Erickson, T. (2017). "Human-Agent Collaboration: Can an Agent Be a Partner?" In: *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '17. Denver, Colorado, USA: ACM, pp. 1289–1294.

Bhudhiraja, R. (2015). "Country Case Studies in ICT for Disaster Management: India".

BRIDGE (2011). "Findings from user interviews".

Büscher, M., Kerasidou, X., Petersen, K., and Liegl, M. (2016). "Code and the City: Regions and Cities". In: Routledge, London. Chap. "Digital Urbanism in Crises", pp. 163–177.

Cook, R. (1998). "How complex systems fail". In: *Cognitive Technologies Laboratory, University of Chicago. Chicago IL.*

Deininger, R. L. (1960). "Human Factors Engineering Studies of the Design and Use of Pushbutton Telephone Sets". In: *Bell System Technical Journal* 39.4, pp. 995–1012.

Dekker, S. (2013). *The Field Guide to Understanding Human Error*. Ashgate Publishing Limited.

Dishaw, M., Strong, D., and Bandy, D. B. (2002). "Extending the task-technology fit model with self-efficacy constructs". In: *AMCIS 2002 Proceedings*, p. 143.

Embrey, D. (2003). *Understanding Human Behaviour and Error*. Tech. rep. Human Reliability Associates.

Glaser, B. and Strauss, A. (1967). *Discovery of Grounded Theory*. Aldine Transaction.

Goodhue, D. L. and Thompson, R. L. (1995). "Task-technology fit and individual performance". In: *MIS quarterly*, pp. 213–236.

Greenbaum, J. (1991). "A Design of One's Own: Towards Participatory Design in the US". In: *DAIMI Report Series* 20.375.

Jentsch, M., Ramirez, L., Wood, L., and Elmasllari, E. (2013). "The Reconfiguration of Triage by Introduction of Technology". In: *Proc. MobileHCI 2013*. MobileHCI '13. Munich, Germany: ACM, pp. 55–64.

Merriam Webster, ed. (2017). *Merriam Webster Learner's Dictionary*.

Mohsin, B., Steinhäusler, F., Madl, P., and Kiefel, M. (2016). "An Innovative System to Enhance Situational Awareness in Disaster Response". In: 13.

Nocera, A. and Garner, A. (1999). "Australian disaster triage: a colour maze in the Tower of Babel". In: *Australian and New Zealand journal of surgery* 69.8, pp. 598–602.

Orthner, H., Mishra, N., Terndrup, T., Acker, J., Grimes, G., Gemmill, J., and Battles, M. (2005). "Information Infrastructure for Emergency Medical Services". In: *AMIA annual symposium proceedings*, p. 1067.

Paul, S. A., Reddy, M., Abraham, J., and DeFlitch, C. (2008). "The Usefulness of Information and Communication Technologies in Crisis Response". In: *AMIA annual symposium proceedings*, pp. 561–565.

Ramchurn, S. D., Huynh, T. D., Ikuno, Y., Flann, J., Wu, F., Moreau, L., Jennings, N. R., Fischer, J. E., Jiang, W., Rodden, T., et al. (2015). "HAC-ER: A disaster response system based on human-agent collectives". In: *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, pp. 533–541.

Rasmussen, J. (1983). "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models". In: *Systems, Man and Cybernetics, IEEE Transactions on* SMC-13.3, pp. 257–266.

Ritter, F., Baxter, G., and Churchill, E. (2014). "Foundations for Designing User-Centered Systems: What System Designers Need to Know about People". In: Springer London. Chap. 2, pp. 33–54.

Sanders, E. B.-N. (1992). "CONVERGING PERSPECTIVES: Product Development Research for the 1990s". In: *Design Management Journal (Former Series)* 3.4, pp. 49–54.

Schmidt, D. J. (2007). *Überörtliche Unterstützung beim Massenanfall von Verletzten: Einsatzkonzept zur Bewältigung von Großschadenslagen mit 500 - 1200 Patienten durch überörtliche Unterstützung. Version 5.0*. Rheinische Projektgruppe "MANV Überörtlich" / BBK Germany.

Seaward, B. L. (2016). *Essentials of Managing Stress*. Jones & Bartlett Learning.

Sklar, E., Schneider, E., Ozgelen, A. T., and Azhar, M. (2014). "Toward Human/Multi-Robot Systems to Support Emergency Services Agencies". In: *2014 AAAI Fall Symposium Series*.

Turoff, M., Chumer, M., Walle, B. V. de, and Yao, X. (2004). "The design of a dynamic emergency response management information system (DERMIS)". In: *Journal of Information Technology Theory and Application (JITTA)* 5.4, p. 3.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). "User Acceptance of Information Technology: Toward a Unified View". In: *MIS Q.* 27.3, pp. 425–478.