Characterizing Incidents Reporting Systems across Applications Domains

Marco Antonio Winckler, Cédric Bach, Regina Bernhaupt

Characterizing Incidents Reporting Systems across Applications Domains

Marco Winckler, Cédric Bach and Regina Bernhaupt

University of Toulouse (UPS), Institute of Research in Informatics of Toulouse (IRIT)
118 route de Narbonne, 31062 Cedex 9, Toulouse, France
{Winckler,cedric.bach,regina.bernhaupt}@irit.fr

Abstract. Incident reporting is a very well-known technique in application domains such as air traffic management and health, where specialized users are trained to provide detailed information about problems. Incident reporting systems are indeed complex systems that include many actors including the users reporting incidents, user's colleagues and neighbors, stakeholders, policymakers, systems integrations. Incident report systems might change (positively or negatively) the users' environment in many ways. In recent years, this kind of technique has been also been used in crisis management such as the hurricane Katrina. However, despite the fact that incident reporting systems using mobile technology are becoming more common, little is known about its actual use by the general population and which factors affect the user experience when using such system. In this paper we discuss the use of incident reporting system in critical context of use. In this paper we discuss the use of incident reporting system in several application domains. In particular we report findings in terms of dimensions that are aimed to identify social and technical aspects that can affect the design, development and use of incident reporting systems.

Keywords: Incident reporting, mobility, geo-localization, user interface patterns, m-government, e-government.

1 Introduction

Incident reporting is a very well-known technique in application domains such as air traffic management [6] and health [7], where specialized users are trained to provide detailed information about problems. What has been found in these areas is that incident reporting is an important means to improve safety by enabling authorities to improve technical systems, design or (work) procedures based on the incident reports. Incident reporting in these safety-critical domains is characterized by being part of the work routine, enabling special benefits for users reporting incidents.

However, in more recent year, incident reporting system has been extended to be used for ordinary people outside of their working settings. In recent years, this kind of technique has been also been used in crisis management such as the hurricane Katrina [11]. Many governments have also started to make use of mobile technology for allowing citizens to report incidents in their neighborhood (e.g. broken street lamps, street water leak) to the local administration [13]. These applications (featuring crowdsourcing systems [3]) are part of a variety of initiatives for promoting active participation of citizens in the actions of the government through the use of information and communication technology (e/m-government) [4][9]. The latest generation of mobiles device include touch interaction, GPS and camera, so that mobile phones (smartphones) provide users/citizens with means to report incidents by specifying location (e.g. typing on a map), sending a precise location (e.g. using GPS) and providing photos or videos of incidents. Such as information enhance the quality of incident descriptions and can be used as proof/evidence such as demonstrated by the applications ispot [5] which illustrates how ordinary people can contribute to conservation initiatives by reporting bird's migration. Thus, despite the fact that incident reporting systems are often associated to safety-critical domains, there is no reason they could not be used to report less critical incidents in users' life.

Nonetheless, reporting incidents in a mobile setting seems to be a quite complex activity as it requires a certain amount of knowledge to describe successfully the observed problem (attributes enabling the identification of the incident itself), time and spatial constraints (ex. incident reporting might not occur by the time/space of the incident itself), privacy issues. Moreover, the importance of these dimensions might vary accordingly to user needs and the application domain. For example, contrary to the work-oriented incident reporting in the safety-critical domain, any mobile phone application for the general public must support the privacy of the citizens/users. In order to analyze the similarities and idiosyncrasies of different implementations of incident reporting system, we propose in this paper a domain space for characterizing incident reporting systems. Such domain space is based on a review of the literature and it provides a synthesis of our previous work on the field [1][14]. In section 2, we start presenting a model-based task analysis of incident reporting systems using mobile phones; this section is aimed to show how generic user tasks can be used to extract a large set of scenarios that can accommodate a large set of scenarios for reporting an incident. In section 3, we discuss a set of dimensions that can influence the decision to implement a particular scenario. Lately in section 4 we present conclusions and future work.

2 Report Incident with Smartphones: Task Model

Task analysis is widely recognized as one fundamental way to focus on the specific users' needs and to improve the general understanding of how users may interact with a user interface to accomplish a given interactive goal [2]. In this section we present a generic task model for incident reporting systems. The main goal of this model-based task analysis is to describe all possible scenarios leading users to successfully report an incident. The current task model assumes the use of mobile phones as a possible target platform for the system.

2.1 Characterization of User Tasks when Reporting Incidents

Despite that incident reports might be virtually used in different situations, let us assume a simple case of incident reporting system allowing a citizen (i.e. a user) to digitally declare, in a mobile context, an urban incident. This activity involves several preconditions: First, a citizen must identify something that matches his mental representation of what is an incident. Mental representations are strongly depended on background, education, cultural values, demographics, involvement, and many other factors. Classical approaches to solve these difficulties should be (a) the clinical approach allowing people to explain their own point of view of an incident, (b) the classification approach providing citizens with a taxonomy from which the users can infer the possible occurrence of an incident (e.g. beach incident category will fit Rio de Janeiro, Cannes, etc. but will not fit Madrid or Washington DC). Second, the citizen must be aware of the existence of the incident reporting service, and then estimate that that service can solve the incident better than any other effort from the citizen him/herself. Third, the citizen must dispose of a device and a service to report the incident.

For the declaration there are three subsequent questions to take into account: What *is an incident?* Several attributes can be used to characterize an incident. It is often mandatory to know where the incident occurred and what its nature is. The localization of the incident is a mandatory attribute to report an incident, even if the location is approximated. If this information is not provided, it will be difficult to solve the incident. Knowing the nature of the incident also helps to solve it more efficiently, so an incident report needs a description (either informal or derived from taxonomy of known types of incidents). *When the incident occurred?* The accuracy of time might differ accordingly to the type of incidents. Whilst some incident reporting will contain exact data and time (e.g. witnessing car crashing) other might be unknown (e.g. when a pothole appears in the lane). The frequency of incidents might also be requested as a mean to better characterize the incident. *Who reports the incident?* Declaration might be anonymous but identification of users reporting incidents might be necessary to prevent spam or trust on the information provided. *How the incident is reported?* Users can describe the incident by writing a note in a paper, sending an email or using a dedicated mobile application featuring a structured form. Devices and technological means will heavily affect the user activity. Technology that supports human memory, provide sense of orientation and the categorization tasks will be useful in this activity. Furthermore, technology is aimed at conciliating space and time between the incident observation and the incident report. At this point, the users have all they need to digitally report an urban incident. To complete the task there would be still the post-condition to this activity. It concerns the feedbacks about the report and refers to the resolution of the incident. This point mainly depends on the back-office activity (e.g. authorities that collect the reports).

2.2 Model-Based Task Analysis

In order to describe the tasks we employ a task model notation called HAMSTERS (Human-centred Assessment and Modelling to Support Task Engineering for Resilient Systems) [8]. Task models described in HAMSTERS feature a hierarchical graph decomposing complex tasks into more simple ones. Tasks are depicted accordingly to the actors involved in the task execution (i.e. the user, the system or both at a time). Complex tasks are called abstract tasks. In additional to hierarchical decomposition of tasks, it is possible to connect two tasks using logical and temporal operators for expressing dependence between task execution (ex. sequence, choice, order independence). Hereafter we only provide the basic constructs of the notation that are necessary for understanding our models. For further information about the HAMSTERS notation please refer to [8]. When reporting an incident the following three main tasks have to be performed: (1) *to detect the incident*, (2) *to submit an incident report* and (3) *to follow up on an incident report*. Figure 1 illustrates the hierarchical organization of these tasks using the HAMSTER notation. The operator >> indicates that these tasks should be performed in a sequence. The execution of the task detect incident is the first step towards incident reporting. Once an incident is detected, users can submit an incident report. As users might edit a report several times before effectively submitting it, this task is set to be iterative (see the left-hand side symbol ⟳). Once it has been sent, the user can follow up an incident report; this task is represented as optional (see right-hand side symbol) as not all citizens will be interested in the outcomes of an incident report.

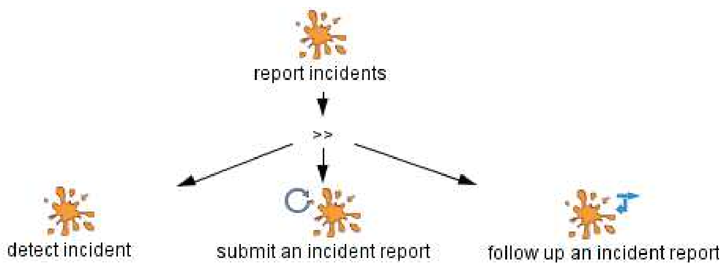

Fig. 1. Main tasks for reporting an incident

Figure 2 provides a more detailed view of user activity by decomposing all complex tasks into more simple ones. Thus the task detect incident is decomposed in several cognitive sub-tasks including the perceptive sub-task recognize an incident and the cognitive sub-tasks identify who should solve an incident and decide to report the incident. These tasks aim at capturing the main issues that occur on the users' side before reporting an incident. For example, to identify who should solve an incident is necessary for determining a system or at least destination for the incident report. Moreover, users should decide [if it is worthy or not] to report an incident. If the user is able to solve these questions he can proceed with the description of the incident.

Generally speaking, the information requested in the identification of the incident includes a description, a location, the time associated to the occurrence of the incident and the identification of the person reporting the incident. Not all this information is mandatory; however at least the description and the location of the incident should be provided. The task “submit an incident” is set as iterative, which means it can be revised until users send the report. It is noteworthy that a user might decide to cancel the submission at any time; this feature is supported by the operator disabling ([>).

Users describe an incident by informing the incident category rating the perceived severity or providing a description for it. For the description, users can perform a textual description, provide a picture/video that shows the problem or incident or call a hot line. The operator |=| indicates these activities can be done in any order. The location of an incident is mandatory; otherwise it would be very difficult to put the means in place to fix it. However, accordingly to the context, users can provide diverse information about the position of the incident: for example by performing the task to provide an address, pinpoint it on a map, use landmarks (ex. in front of the Eiffel tower) or solve GPS coordinates. A report can be completed by adding optional information about the time and the user. In some situations, users are able to report the time for the incident, which implies the user task tell when the incident occurred and the system task record when the incident is reported. The sub-task report time for the incident is optional because it is very likely that incidents occur without any witness so that the exact time for an incident is unknown.

Users might be requested to provide personal identification either by identifying themselves or allowing the system to use personal coordinates already known by the system (ex. cellphone number). Identification of users can vary considerably from a system to another. Precise user identification might help to prevent spam and false reporting, or to contact users if needed. However, we shall notice this is a requirement for the authorities, not for the users. Indeed, incidents description might remain accurate and valid even if reported anonymously. After submitting a report, some users might want to follow up an incident report. It is worth noting that the subscription for a notification might also engage users in a communication with the back-office. Some users might also want to share reports using a social network or just be interest in to see reports sent by others users. Of course not all users will follow up an incident report so closely, so this and all subsequent sub-tasks are described as optional. The task model presented in Figure 2 provides a comprehensive view of tasks related to incident reporting; however it does not impose any particular design for the system. Using the simulator embedded into the HAMSTER editor it is possible to extract 122 alternative sequences of tasks leading to the same goal. For example, from our task model we could extract a simple scenario that requires very few information through basic text fields to report an incident. Another scenario extracted from the model integrates tasks allowing users to provide pictures for the incident and allowing the system to solve GPS coordinates that will be automatically added as part of the incident report. We assume that by extracting the appropriate scenarios from this task model we are able to describe a large set incident reporting in various applications domains such as health, ATM, e/m-government.

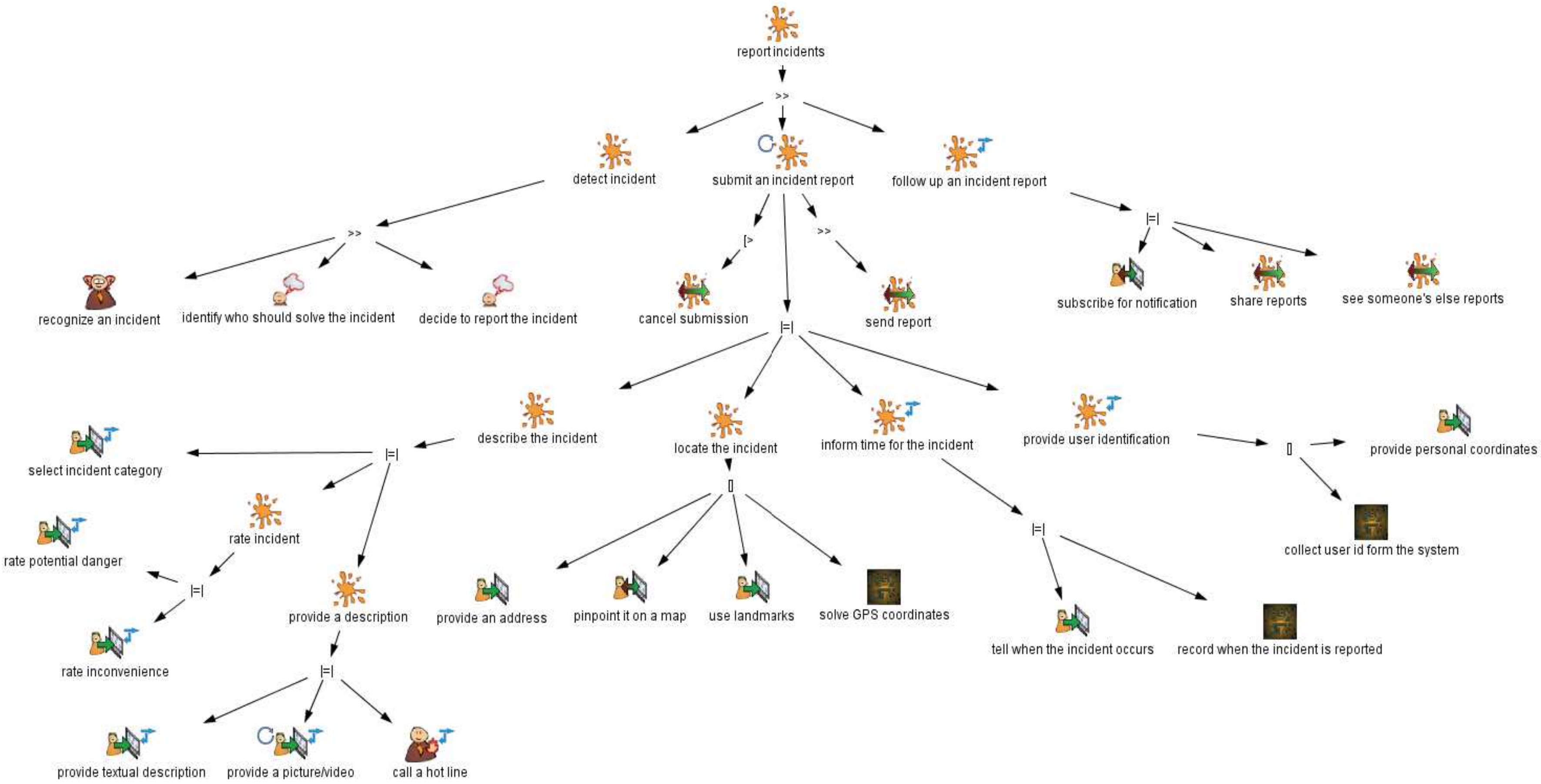

Fig. 2. Generic task model for reporting an incident

3 Dimensions Characterizing Incident Information Systems

This section presents a set of dimensions for characterizing incident reporting systems. These dimensions are heavily inspired from the task analyzed presented in previous sections but also from our previous work [1][14] and review of the literature, in particular [10][12]. Table 1 provides a view at glance of the dimensions including possible values for each category.

Table 1. Domain space for incident reporting systems

Incidents characteristics	**Type**	uncategorized	user's categorization	Taxonomy	
	Severity	minor incident	important	dangerous	safety-critical
	Inconvenience	none	low	medium	high
	Location	address	GPS coordinates	contextual location	moving incident
	Frequency	one shoot	recurrent	event based	unpredictable
	Duration	undefined	punctual	fixed duration	evolving
	Level of accuracy	informal description	structured description	evidence (photo)	certified report
Users characteristics	**Identification**	Anonymous	profile	role	person
	User's involvement	none	observer	witness	responsible for
	User's motivation	none	low	medium	high
Technology	**Technologies**	paper	desktop application	Website	smartphone application
	Outcomes	no feedback	system acknowledgment	personalized feedback	follow up incident
	Proactivity	no prompt	help	safeguarding	prompting

3.1 Incident Characteristics

The following dimensions are used to define the characteristics of an incident:

- The *type* of an incident concerns a graduation of incidents categorizations that would be used to classify incidents. This follows a scale that ranges from less accurate to more accurate categorizations: *Uncategorized incident*, *Incident categorized directly by users* and finally using *taxonomy of incident* types.
- *Location* refers to the different means and characteristics of incident location. The localization of the incident is a mandatory issue to report an incident. If this issue is not completed, it will almost be impossible to solve the incident. This dimension also follows a graduation: address, GPS, contextual location and finally a moving incident (e.g. a stray dog).

- *Severity*. We assume that users differentiate incidents with different degrees of severity ranging from a minor incident to dangerous incidents. The report of a minor incident will generally be driven by the perception that it is a users' duty.
- *Inconvenience*. The level of inconvenience is characterized by the troubling nature of the incident either from an organizational point of view or in terms of moral or material values. Inconvenient incident may damage equipment or disturb the peace. It would be range from *none* inconvenience to variable scale that is illustrated here as *high inconvenience*.
- *Frequency* is a temporal dimension aiming at defining the repetition of an incident. Possible values include *one shoot* (single occurrence), *recurrent* id users said that this is not the first time it occurs, *event based* when users are able to identify the event that triggers the incident, and or *unpredictable.*
- *When the incident occurs*. This is another temporal dimension. Possible values for duration might include: *undefined* when users cannot tell it, *punctual* when the date/time can be determined as a unit of time, *fixed duration* when users can inform the beginning and the end of an incident, and *evolving* when the incident is a continuous event that users cannot inform either the start and/or the end.
- *Accuracy* refers to the quality of the information in an incident report. Possible values are *informal description* of an incident*,* clear and *structured description* (possibly characterizing all attributes of an incident), *and evidence* such as photos or factual data provided by the users, and *certified report* when users can provide a proof of the occurrence of the incident or when the user is a certified expert whose reports are legally trusted by authorities.

3.2 Users Characteristics

The following dimensions characterize the users that report an incident:

- *Identification* refers to which extension a person can be associated to an incident report. For example, the report can be *anonymous*, identified by a *user profile* such as a young/elder user, a *role*, the attributes such as name, sex, addresses that provides a clear identification of a *person*.
- *User's involvement in the incident* describes the particular role of a user in the incident such as *observer, witness* or *responsible for* the incident.
- *User's motivation* might encompass one of the following: (a) identification of an event that could be perceived as a nuisance/problem, (b) detection of an event that could prevent the occurrence of an likely nuisance/problem, and (c) identification of something worthy reporting that could improve the quality of the environment and/or its management. The detection of an incident is based on tangible characteristics identified in the environment and how an individual interprets them in the respective location. The perception of an individual of the nature of an incident appears to have an impact on its level of involvement in the reporting process, it also influencing the time and the number of operations a user is willing to spend and to perform an incident report.

3.3 Technology

Technology covers three main dimensions that characterize the technological means used with incident reporting systems.

- *Technologies*. This dimensions includes the diversity of platforms (e.g. Android, iPhone, Windows Phone,...) and the types of communication means (i.e. direct interaction as on desk in a city hall, use of paper forms, synchronous communication such as in phone call or asynchronous as in text message) seems to affect the effective use of incident report systems. This dimension follows a graduation of different technical means as desk, paper forms, website, and smartphone application.
- *Outcomes* refers to the type of feedback users can get after reporting an incident. It might include: *no feedback, system acknowledgment, personalized feedback* and the possibility for a user to *follow up incident*.
- *Proactivity* refers to the level on which the system implements features for prompting users to report incidents. Possible values are: *no prompt, help* is provided when users ask for it, *safeguarding* users from performing dangerous tasks, or *prompting* when the systems explicitly request users to provide information.

4 Discussions and Future Work

Incident reporting systems can be used in different context such as reporting problems in working setting, promote citizens involvement with governmental initiatives, monitoring the environment, etc. In this paper we have discussed dimensions involved in incident reporting activity. We have presented a task model from which we can extract a large set of scenarios that can accommodate many types of incident reporting systems. Moreover, we have provided a preliminary domain space model with the main dimensions that can be used to tune the profile of scenarios supported by incident reporting systems. By extracting the appropriate scenarios and using the values associated to which dimension of the domain space we are able to characterize a large set of incident reporting systems. This is first step leading to the comparison between different incident reporting systems across application domains.

We also have discussed several concerns that should be taken into account when designing the user interface. Our results are very preliminary but they raise several questions of both scientific and practical significance: what are the user needs for reporting incidents? What are the dimensions and how do they affect the user experience when reporting incidents? How to reduce training with the user interface for reporting incidents and still provide accurate description of problems? How to handle localization issues on urban context of issues? How to cope with temporal constraints related to the occurrence of the incident and the time of reporting it? What is the minimal information for identifying incidents? What is the role of social networking activities in policing incident reports? How to compare incident reporting systems used for different purposes and in different application domains? Can design solutions for reporting incidents in a domain be transferred to another application domain? How mobile technology might affect users' tasks for reporting incidents?

The present work is a first step forwards the identification of best (and bad) practices for the design of user interface of critical incidents. Most of the analysis held in the current paper is based on user requirements and analysis of user tasks. Our future work will include the validation of the dimensions of the information space with more real case studies. The goal is to make sure that none dimension necessary to characterize the information space was let out.

Acknowledgments. This work is part of the Ubiloop project partly funded by the European Union. Europe is moving in France Midi-Pyrenees with the European Regional Development Fund (ERDF). Genigraph and e-Citiz are partner of this work.

References

1. Bach, C., Bernhaupt, R., Winckler, M.: Mobile Incident Reporting in Urban Contexts: Towards the Identification of Emerging User Interface Patterns. In: 5th IFIP's WG 13.2 Workshop PUX, Lisbon, Portugal, September 5 (2011)
2. Diaper, D., Stanton, N.A. (eds.): The Handbook of Task Analysis for Human-Computer Interaction, 650 pages. Lawrence Erlbaum Associates (2004)
3. Doan, A., Ramakrishnan, R., Halevy, A.Y.: Crowdsourcing systems on the World-Wide Web. Commun. ACM 54(4), 86–96 (2011)
4. El Kiki, T., Lawrence, E.: Mobile User Satisfaction and Usage Analysis Model of mGovernment Services. In: Proc. of Euro mGov 2006: Second European Conference on Mobile Government, Brighton, UK (2006)
5. ispot (2012), http://www.ispot.org.uk/
6. Johnson, C.W.: Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting. University of Glasgow Press, Glasgow (2003)
7. Kaufmann, M., Staender, S., von Below, G., Brunnerc, H., Portenier, L., Scheidegger, D.: Déclaration anonyme informatisée d'incidents critiques: une contribution à la sécurité des patients. Bulletin des Médecins Suisses 84 (2003)
8. Martinie, C., Palanque, P., Winckler, M.: Structuring and Composition Mechanisms to Address Scalability Issues in Task Models. In: Campos, P., Graham, N., Jorge, J., Nunes, N., Palanque, P., Winckler, M. (eds.) INTERACT 2011, Part III. LNCS, vol. 6948, pp. 589–609. Springer, Heidelberg (2011)
9. Misuraca, G.: Futuring e-Government: governance and policy implications for designing ICT-enabled Knowledge Society. In: Proc. ICEGOV 2009, Bogota, Colombia (2009)
10. Moon, J.: From e-Government? Emerging practices in the use of m-technology by state governments. IBM Center for the Business of Governement (2004)
11. Moynihan, D.P.: From Forest Fires to Hurricane Katrina: Case Studies of Incident Command Systems. IBM Center for the Business of Government (2007)
12. Reason, J.T.: Human Error: models and management. Br. Med. J. (2000)
13. Song, G.: Transcending e-Government: a Case of Mobile Government in Beijing. In: Proc. of The First European Conference on Mobile Government, Sussex (July 2005)
14. Winckler, M., Bach, C., Bernaupt, R.: Identifying User experiencing factors along the development process: a case study. In: Proc. of Int. Workshop on the Interplay between User Experience Evaluation and System Development, I-UxSED 2012, Copenhagen, Denmark, October 15 (2012)