A framework for interoperability assessment in crisis management

D. da Silva Avanzi [a,b], A. Foggiatto [a], V.A. dos Santos [a], F. Deschamps [a,*], E. de Freitas Rocha Loures [a]

[a] Industrial and Systems Engineering Graduate Program, Polytechnic School, Pontifical Catholic University of Parana, Rua Imaculada Conceição, 1155, 80215-901 Curitiba, PR, Brazil
[b] Instituto das Cidades Inteligentes, Rua São Pedro, 910, 80035-020 Curitiba, PR, Brazil

ARTICLE INFO

ABSTRACT

It is noticeable the growth of various types of concerns in large centers, whether by citizens or public officials. In that sense, an important dimension is crises management such as in cases of natural disasters. This scenario calls for a task force in an attempt to predict or solve emergencies, especially in managing and integrating public and private spheres, which in turn are centered on public authorities, service providers, citizens, volunteers and systems. In order to allow the exchange of information and joint actions of those involved entities, the fulfillment of interoperability requirements becomes a critical factor to promote improved performance of the actions taken in these situations. Based on the literature and related worldwide initiatives, the main concerns and attributes of crisis management are identified from the perspective of interoperability. Founded on this knowledge a framework that supports a Disaster Response Management System (DRMS) development cycle is proposed focusing on a diagnostic step based on a multi-criteria decision analysis techniques (MCDA) to assess potential interoperability of a public entity or locality. The proposed MCDA method facilitates the specification of integrated solutions for the public sector to meet interoperability requirements in disaster management (DM) scenarios. In this paper the assessment method was based on the Analytic Hierarchy Process technique (AHP), and applied to a company involved in the DM domain, responsible for the information technology infrastructure of a city in the south of Brazil. The findings show the main gaps of the entity under the interoperability perspective, allowing the identification of key areas for improvement of its DM capabilities coherent to the DRMS deployment process.

1. Introduction

Regardless of its nature, a crisis is considered an abnormal situation, usually resulting from an instability that impacts a part of society with unacceptable consequences. A crisis situation can emerge in different contexts - political, military, economic, humanitarian, social, technological, environmental or healthcare. Lately, it is noticeable that authorities are increasingly seeking solutions to improve the management of crises. Part of this growth is due to increased citizen participation. Through the ubiquitous use of technology, people are both more collaborative in crisis moments and demanding more transparency by closely monitoring measures taken by the responsible [1].

In this sense, crisis management is becoming more and more relevant. Managing a crisis involves the participation of various entities working together in an action cycle based on four main phases: mitigation, preparedness, response and recovery [2]. The response phase is both relevant for meeting performance requirements and critical for the support that may be provided to any impacted group of individuals. Efficiency in managing a crisis is measured by the speed and precision with which information is managed and exchanged among partners (i.e., organizations, people, and devices involved in the collaboration). This efficiency and performance therefore depend not only on information systems, but on associated dimensions such as strategy, processes, services and roles that guide the coordination of the entities involved. Thus, successful crisis management, particularly in response actions, requires full integration of all of the involved parties through different inter and intra-organizational concerns [3].

It is possible to analyze the management of a crisis considering the viewpoints of two important entities directly involved in this kind of unexpected situation - firefighters and police officers.

* Corresponding author.
 E-mail addresses: davanzi@ici.curitiba.org.br (D.d.S. Avanzi), afoggiatto@yahoo.com.br (A. Foggiatto), vanessapolly_@hotmail.com (V.A. dos Santos), fernando.deschamps@pucpr.br, fernando.deschamps@terra.com.br (F. Deschamps), eduardo.loures@pucpr.br (E. de Freitas Rocha Loures).

For instance, in the case of notification of a large crash on a highway, information usually arrives simultaneously at more than one police or fire departments without proper control and information sharing. This results in more than one rescue team being sent to the scene and impairs mobility due to the concentration of rescue vehicles. This scenario may be even more complex when involving more extreme environments, such as the seas and oceans [4]. This highlights the importance of information exchange and integration of different services involved in providing response to an incident and shows the relevant role interoperability among these entities plays in these situations.

Interoperability can be defined as a broad concept encompassing the ability of entities (e.g., organizations or systems) to work together in pursuit of common, mutually beneficial goals. Thus, if two or more entities do not have the ability to collaborate, exchange information and coordinate actions, they cannot be considered interoperable [5]. For entities to become interoperable, they must meet certain common goals and requirements, which in turn must be set according to their application domain.

To identify their capabilities to interoperate, entities should be subject to an assessment, which allows stressing out how a particular entity is interoperable in its application domain. This refers to the definition of potential interoperability [6], particularly related to the crisis management domain, characterized by complex dynamics involving a priori undefined knowledge about entities expected to interoperate. The potential interoperability assessment represents an appropriate diagnostic tool for mapping the elements of influence on the efficiency and performance of involved entities. It should assist in identifying and reviewing technical and managerial requirements of entities' information systems and considered by a disaster management project lifecycle as advocated by Noran [7].

This paper presents a Disaster Response Management System (DRMS) development cycle framework with a focus on a diagnosis step devoted to potential interoperability assessment of a public/private entity or locality. The proposed approach uses a multi-criteria decision analysis structure based on AHP (Analytic Hierarchy Process) and helps organizations perceive their strengths and weaknesses, devising actions closely related to their ICT capabilities to increase performance and maturity. The diagnosis results support the specification of a DRMS that fulfills interoperability requirements coherent to entity capabilities in disaster management.

The paper is structured as follows. Section 2 presents the main worldwide initiatives, as well as the literature review to investigate performance perspectives and the effectiveness of the actions taken in disaster management together with the principles of interoperability. Section 3 describes the interoperability assessment model for crisis management considering all the artifacts used in its development supported by a specific framework. In Section 4 the assessment model is applied to a real case, allowing the evaluation of a given entity and its environment regarding its interoperability capabilities. The company responsible for Curitiba (southern capital of Brazil) municipal information technology infrastructure was chosen as an application case. Finally, in the conclusion section, the main outcomes, lessons learned and research perspectives are presented.

2. Scientific scenario and related works

2.1. Disaster management

There are three main aspects to be considered in managing disasters - protection of life, property and the environment. Disasters are usually classified into natural or man-caused. The former are related to events such as earthquakes, floods, storms, hurricanes, tornadoes, cyclones and forest fires. The latter covers events such as the collapse of buildings or accidents involving air transportation. Regardless of the type of disaster, achieving an effective and coordinated action is a difficult task for first responders [8].

The different rescue organizations such as police and fire departments, health services, civil defense and others must be efficient when working in a collaborative way, considering the inter and intra-organizational aspects, in addition to the different hierarchical levels of each involved team [3]. Thus, the exchange of information becomes an essential prerequisite for dealing with the different types of disasters in a fast and coordinated manner. Proper management and integration of participants is required in enabling the exchange of information targeted at prevention or mitigation of crisis situations [1]. Thus, the whole operation requires that information is kept as up to date as possible, requiring real-time communication between participants.

Such exchange of information may be easy to solve in some cases. But the problem can grow larger when a need for crisis control and recovery covers areas with greater difficulty in communication and access. One can mention wild environments and marine areas, that require adequate measures to minimize the damage caused by, for instance, an earthquake, especially in financial matters and life protection. To face this scenario, Wang and Tanaka [4] propose a system for optimizing the marine logistics in case of emergency or disaster (earthquake) by assigning ships to transport routes, considering all possible adversities imposed by this scenario.

Far from extreme environments, companies are also concerned with managing disasters. Some authors [9,10] describe the factors of influence that increase the risks for such disasters, as environmental, logistical and external catastrophes, always proposing recovery methodologies. For instance, a supply chain risk assessment methodology to face disaster response requirements is proposed [9]. Although the model presented by the author suits the industrial context, it can also be adapted and applied to other domains. Such a model aims to improve resilience through matrices that confront samples of different disturbances that have led to different types of supply chain failures. These scenarios, whether in extreme environments or not, require greater care in order for communication to occur efficiently.

The real-time exchange of requirements in a crisis scenario drives the need to integrate information and communication technology systems (ICT) in delivering disaster management support, providing efficient and safe exchange and processing of information [3]. Most collaboration and communication issues in companies are supported by Information Systems (IS) without capabilities to face process coordination and information flows among heterogeneous entities and systems. The implementation of a Mediation Information System (MIS) supported by a Service Oriented Architecture (SOA) represents an interesting solution allowing an evolutionary monitoring of the crisis scenario, and the management of information among entities involved [11].

Thus, in the field of emergency and disaster, Crisis Information Management Systems (CIMS) or Disaster Management Interoperability Systems (DMIS) have been part of the prevailing concept in use in real cases as proposed in [12,13]. Their main objective is to provide a complete set of ICT functions to address many needs of the players in crisis management. CIMS has been highlighted as a preferred system by entities to meet the main needs of crises situations, in particular, the exchange of information, enabling efficient joint and coordinated actions by those involved [12]. Multiple cross-organizational actions are performed by these types of systems [14]: ongoing assessment throughout the crisis period; start, maintain and control communications; identify the incident management strategy; decision-making based on resources available; request additional resources; develop an organizational command