A Modeling Framework for Evaluating Effectiveness of Smart-Infrastructure Crises Management Systems

Tridib Mukherjee and Sandeep K. S. Gupta
Impact Lab, Department of Computer Science and Engineering
School of Computing & Informatics
Arizona State University, Tempe, AZ 85287
http://impact.asu.edu
sandeep.gupta@asu.edu

***Abstract*—Crises management for smart-infrastructure – infused with sensors, actuators, and intelligent agent technologies for monitoring, access control, and crisis response – requires objective and quantitative evaluation to *learn for future*. The concept of *criticality* – characterizing the effect of crises on the inhabitants of smart-infrastructure – is used in this regard. This paper establishes a *Criticality Response Modeling (CRM)* framework to perform quantitative evaluation of criticality response. The framework can further be incorporated in any criticality-aware middleware for smart-infrastructure. An established stochastic model for criticality response is used from our previous work. The effectiveness of criticality response is measured in terms of the *Manageability* metric, characterized by the *Q-value* or *Qualifiedness* of the response actions. The CRM is applied to fire emergencies in an envisioned *smart* Oil & Gas Production Platforms (OGPP). A simulation based evaluation, using CRM over OGPP, show that high manageability is achieved with – i) fast criticality detection, ii) fast response actuation, and iii) non-obliviousness to any subsequent criticality during response actuation – verifying the applicability of Q-value as the manageability metric.**

***Index Terms*—Crisis Response, Criticality, Stochastic Model, Smart-Infrastructure, Evaluation Framework, Middleware, Human-centered computing**

I. Introduction

Crises management is a challenging problem for homeland security. Typically, crises management encompasses four phases of operation [1]: 1) immediate *response* to the crisis for protecting lives and property, 2) *recovery* efforts in the aftermath of the crisis, 3) *mitigation* to lessen the impact of the crises, and 4) *preparedness* to learn from the outcome for future crises. Figure 1 depicts a simple scenario in which a fire breaks out (crisis) in a building and demonstrates how crisis management should enable adaptive response and recovery involving possible human activities (e.g. fire-fighters and inhabitants). Lessons learned from the 9/11 terrorist attacks and the natural disasters such as Katrina, call for better *preparedness* for such crises to effectively handle them [2]. It is essential to learn from the outcome of previous crises response to improve the preparedness [1]. Evaluating the *effectiveness* of crises response processes is therefore of utmost interest in this regard to verify the outcome (Figure 1). Attempts to develop standard evaluation criteria for crisis management have generally resulted in cumbersome documents such as reports/recommendations, personnel training, and so on [1].

These qualitative measures, although important for the analysis of the crises and their aftermath, are inadequate for a smart-infrastructure – infrastructure infused with sensors, actuators, and intelligent agent technologies [3] – which require *quantitative measures* and procedures for their evaluation. Further, the existence of the automated agents can overlap the actions for mitigation (termed as the *mitigative actions*) with the crises response – requiring different evaluation framework for crises management in the smart-infrastructure. The rest of the paper interchangeably uses the terms "response action" and "mitigative action". The effect of crises to the inhabitants of a smart-infrastructure has been characterized as ***criticality*** in our previous work [4]. Although criticalities are unpredictable, they are not unexpected [1], and depend on the occurrences of the causing critical events (Figure 1). A state-based stochastic model has been established to capture the probable criticalities and the corresponding response actions' effectiveness [4]. The theoretical foundation presented in [4] characterizes the effectiveness as *Manageability*, measured in terms of *Q-value* or *Qualifiedness* of the response actions. *However, a cohesive framework binding the response processes to the theoretical model to evaluate real-life emergency response processes is missing*.

The *goal* of this paper is to *develop a generic modeling framework*, which uses the established stochastic model to evaluate the effectiveness of crises response. In this regard, there are three major contributions of the paper:

1) Development of **Criticality Response Modeling (CRM)** framework to evaluate criticality response effectiveness.
2) Application of the CRM framework on fire emergencies in the Oil & Gas Production Platforms (OGPP).
3) Simulation based verification by evaluating the fire emergency response process using CRM over OGPP.

The CRM framework can be incorporated in any context-aware middleware [5] for handling criticalities in smart-infrastructure. Results show that manageability is inversely affected by – i) the criticality detection delay, and ii) the response actuation delay. This verifies the applicability of Q-value as the manageability metric. CRM further allows comparison between

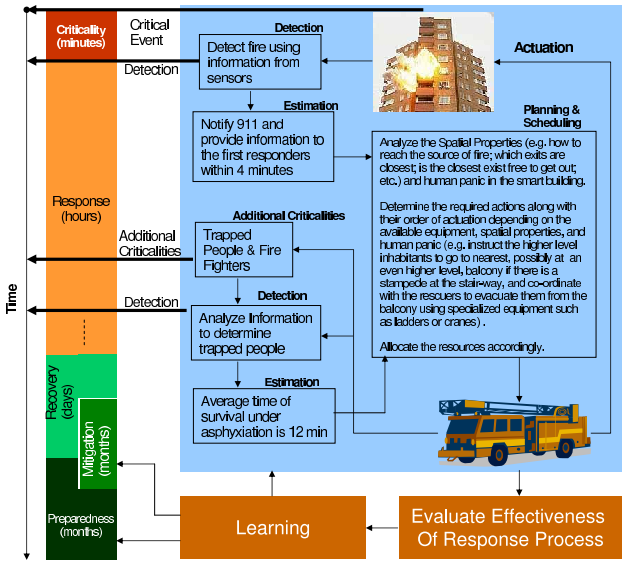


Fig. 1. Criticality management under fire break-out in a smart building

different criticality response action selection policies – enabling automated learning and crises preparedness. In this regard, two different action selection policies – i) *Greedy*, which selects the response actions based on the actions' success probabilities; and ii) *Mitigative Action based Criticality Management (MACM)*, which selects the actions to maximize the Q-value [4] – are compared for fire emergencies in OGPP. It is verified that actions, oblivious to any subsequent criticality, lead to lower manageability – further validating the use of Q-value as the manageability metric.

II. Related Work

A large number of research has been geared towards the design, development and evaluation of computing systems for crises response. Examples include – i) a multi-modal data gathering and dissemination platform being investigated by the RESCUE project [6]; ii) a provisioning tool for resource allocation and decision making for the Emergency Managers envisioned by the Secure-CITI project [7]; and iii) a resource management system for multi-crisis handling in urban settings [8].

Performance evaluation of such systems is essential to ensure service availability during crises. Evaluation of large-scale reliable distributed computing systems for any "sense-and-respond" applications including crises management [9] has been performed in terms of *timeliness* and *appropriateness* of response actions [10]. The advent of safety-critical systems (e.g. heart pacemaker and computer networks in modern cars) enabled in-depth research [11] to evaluate these systems in terms of operational reliability avoiding failures during crises [12] [11].

As opposed to these approaches, *this paper focuses on developing an evaluation framework for the entire crises response process in smart-infrastructure encompassing – i) physical, ii) human, and iii) computational components*. To this effect, the Criticality Response Modeling (CRM) framework is proposed based on – i) the concept of *criticality*, characterizing crises in smart-infrastructure [13] [4]; and ii) an established stochastic model for criticality response [4].

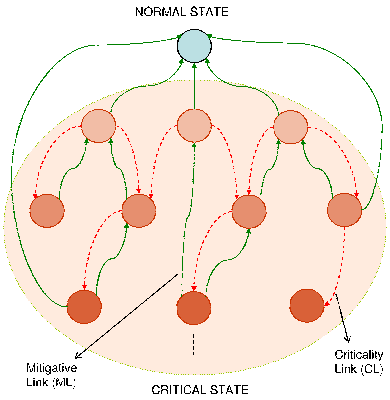


Fig. 2. Critical State Transition Diagram

III. Criticality Response Modeling (CRM) Framework

This section proposes the Criticality Response Modeling (CRM) framework for evaluating criticality response effectiveness. We begin with a brief overview on *criticality* and the state based stochastic model [4] followed by the CRM framework.

A. Criticality: Concepts and Characteristics

The changes in the smart-infrastructure and its environment, which lead the system into a disaster (such as loss of lives and/or property) are called ***critical events*** [4]. **Criticalities** are the effects of the critical events on the smart-infrastructure. It should be noted that by definition, criticalities lead to disasters if proper and timely response actions are not performed. The timing requirement associated with a criticality is referred to as the *window-of-opportunity* for the criticality [13] [4]. Detection of criticalities and actuation of the response actions have to abide by the corresponding window-of-opportunities of the criticalities in the smart-infrastructure.

To this effect, a verifiable property of criticality management called *Responsiveness* is identified and analyzed in [4]. Responsiveness characterizes the speed with which the smart-infrastructure initiates the critical event detection. A **controllability condition** is established based on the temporal properties of criticalities. This condition encompasses the level of responsiveness to give an upper bound on the time taken for detecting and responding to the critical events. The higher the responsiveness the more time there is to take the response actions [4].

The effectiveness of criticality response is further characterized in terms of **Manageability**, which depends on the controllability condition and the uncertainties involved in performing the response actions due to possible human involvement.

B. Stochastic model for criticality response

A state-based stochastic model to characterize criticality response is established in [4]. Smart-infrastructure under one or more criticalities is in the critical state, otherwise it is in normal state. Figure 2 depicts a hierarchical organization of the critical states. A critical event takes the system down the hierarchy through the downward links – also termed as the *Criticality Links (CLs)* (Figure 2). Response actions, on the other hand, take the system up the hierarchy toward the normal state through

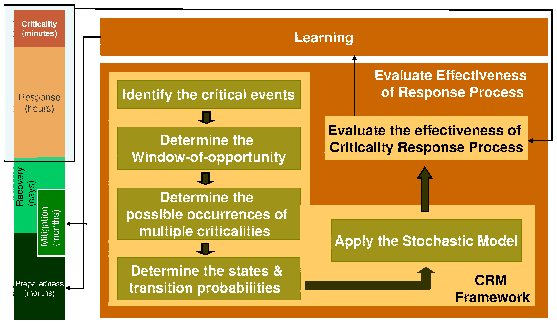


Fig. 3. Modeling Framework for Criticality Management

the upward links – also termed as the *Mitigative Links (MLs)* (Figure 2). CLs and MLs further associate with a probability [4]. The probabilities associated with the CLs signify the probabilities of the corresponding criticalities' occurrences. The probabilities associated with the MLs signify the probabilities of the corresponding response actions' success.

The manageability of a criticality response process is measured in terms of *Q-value* (determining the *Qualifiedness* of the response actions) achieved by the selected actions from a critical state [4]. The Q-value is defined as the probability of reaching the normal state based on: 1) the individual link probabilities of the selected response actions (i.e. the probabilities associated with the corresponding MLs), 2) probabilities of additional criticalities while taking the actions (i.e. probabilities associated with the CLs originating from the intermediate states), and 3) conformation to the controllability condition [4].

C. Framework for evaluating criticality response

Given the definition of criticality, and the foundation for determining the manageability of criticality response, we now present the CRM framework, which binds the real-life crises response processes to the stochastic model. The framework enables: i) evaluation of the effect of detection and response actuation delays on the manageability; and ii) comparison of the outcome of different response action selection policies. Figure 3 elaborates "Evaluate Effectiveness of Response Process" of Figure 1, using the CRM framework to apply the stochastic model to evaluate the effectiveness of criticality response processes. As depicted in Figure 3, the proposed CRM framework consists of five principal components:

1. Identification of the Criticalities: First and foremost, the criticalities are identified based on the possible outcomes of the causing critical events.

2. Determination of the Window-of-opportunities: Secondly, the window-of-opportunity associated with the identified criticalities are determined. This is achieved through experimental study and statistical analysis from previous occurrences of similar critical events. Further, the window-of-opportunity can be situation dependent, and therefore can depend on the existence of simultaneous criticalities as well as the response actions selected for those criticalities.

3. Determination of critical states: The critical states are determined based on the identified criticalities and the possibilities of their concurrent occurrences.

4. Determination of critical state transition probabilities: The probabilities associated with the CLs are derived from the possible human error probabilities that lead to additional criticalities. The probabilities associated with the MLs are derived from the successful completion probability of the actions. Similar to the window-of-opportunity determination, this process also depends on the statistical analysis and human behavior modeling under the crises situation.

5. Application of the stochastic model: Once the critical states are identified and their transition probabilities are determined, the stochastic model can be used to calculate the Q-value for any selected set of response actions for any set of criticalities.

The CRM framework can be used in any criticality-aware middleware for the smart-infrastructure. The entire criticality response process is evaluated based on how much time is taken to perform the selected set of response actions and the transition probabilities associated with the corresponding MLs. The Q-value of the selected set of actions determine the manageability in the range $[0, 1]$. Such evaluation enables quantitative analysis of the outcome of the criticality response process based on the effect of the actuation delay of the selected actions and the criticality detection delay. Additionally, two different set of action selection policies can be compared for a better learning process improving the preparedness of crises management.

The following section uses the CRM framework on a real crisis situation – fire emergencies in offshore Oil & Gas Production Platforms (OGPP) – based on which the aforementioned claims are verified in Section V.

IV. Fire Emergency in Oil & Gas Production Platforms (OGPP)

We commence by briefly describing the emergency response process. Figure 4 depicts a sample flow of events and actions during fire emergency management in the OGPP. An alarm is set off in the OGPP under fire and explosion. In case an imminent danger is ascertained (i.e. the alarm is not a false alarm), the workplace is made safe by taking all the equipments to the safe state. In this way, any possible spread of fire and explosion due to chemical elements used in the equipments are avoided.

Apart from this, the personnel (if any) are egressed (evacuated) based on an evaluation of the possible evacuation paths. The evacuation paths are later assessed to affirm the tenability. If in certain situations (such as spread of fire) the quality of the evacuation path deteriorates an alternate route is chosen for evacuation. The evacuation process further involves i) collection of personal survival suits, and ii) assisting other personnel if needed (or as directed). At the end of the evacuation, the evacuees are registered at a temporary refuge. It is obvious that once this stage is reached, the danger to the evacuees' lives is averted. This recovery process further includes the action of making the equipment safe and giving feedback for proper learning and preparedness to the future fire emergencies.

However, such feedback is subjective and therefore is inadequate for smart-infrastructures, envisioned for OGPP in this paper. Embedded devices (sensors, handhelds, home automation systems etc.) and automated agent technologies can be deployed to enable evaluation and facilitation of the emergency response. This paper applies the CRM framework for an objective evaluation of the fire emergency response. This will enable better learning capabilities of the automated agents based on the quantitatively measured outcome of the response actions.

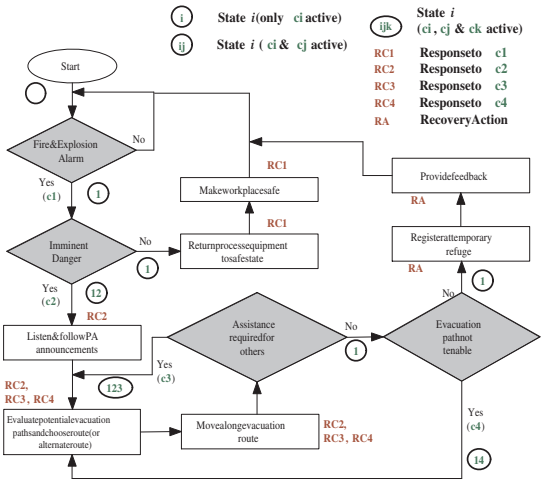


Fig. 4. Flow of actions for fire emergencies in OGPP and the mapping of the criticality response process to MACM framework.

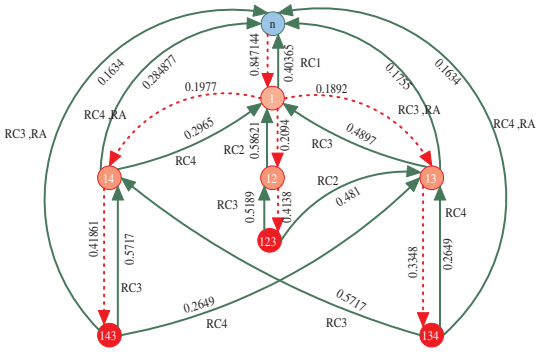


Fig. 5. State transition diagram for the criticalities and response actions in the scenario of fire and explosion in OGPP.

A. Applying the CRM Framework

1) Identify the Criticalities: The *'yes'* branches going out of the decision boxes (shaded diamonds) in Figure 4 are mapped to different criticalities. Accordingly, the set of criticalities in case of a fire emergency in OGPP is summarized below:

- **Criticality 1** ($c1$): Alarm for fire and explosion.
- **Criticality 2** ($c2$): Imminent danger (such as health hazards to the building inhabitants) under fire and explosion.
- **Criticality 3** ($c3$): Persons getting trapped due to spreading of fire and explosion.
- **Criticality 4** ($c4$): Evacuation path is not tenable.

2) Window-of-opportunity for the criticalities: The average time for survival of people under asphyxiation (which happens due to fire and explosion) is 12 minutes. Criticalities $c1$, $c2$, and $c3$ therefore have window-of-opportunities of 12 minutes each. The window-of-opportunity of $c4$ also depends on the time taken to find out the tenability of the evacuation route. The time taken to determine the tenability of the evacuation route is same as the time to perform evacuation through the route (i.e. the response action time for $c2$) [14].

3) Critical States: The last three criticalities ($c2$, $c3$, and $c4$) can occur only as a consequence of the first criticality ($c1$). Figure 5 shows the critical states reached due to the occurrences of the criticalities. State n is the normal state. Any other state of the form i, ij, and ijk denotes the situation where c_i is active, c_i & c_j are active, and c_i & c_j &c_k are active respectively. Note here that the flow-chart in Figure 4 shows a sequential view of the criticalities and their handling. In reality, there can be different sequences in the occurrences of criticalities as captured in the state transition diagram in Figure 5. For example, it might be possible that after the fire alarm is set off (i.e. criticality $c1$ occurs) it is evaluated that the evacuation paths are not tenable (i.e. criticality $c4$ occurs), leading to the possibility of state 14.

4) Critical State Transition Probabilities: Each ML in Figure 5 associates with a label which maps the actions in Figure 4. The response actions for $c1$ includes returning process equipments to safe state and making the workplace safe. The response action for $c2$ is the evacuation of people through chosen routes. Upon occurrence of $c3$, additional people are assisted in their evacuation. Criticality $c4$ requires response such as evacuation through different route to avoid any disaster.

The precise human error probabilities, which determine the probabilities of successfully completing the mitigative actions and the probabilities of any subsequent criticalities, have been estimated in [14]. These estimations are used to determine the probabilities associated with the MLs and CLs. The calculation of probabilities for CLs is performed by taking a product of the error probabilities that lead to the criticalities. The probabilities for MLs are calculated by taking a product of success probabilities (subtracting the error probabilities from 1) of all the actions associated to the corresponding responses. In case of the states with multiple simultaneous criticalities the probabilities of all the outgoing links are further normalized such that they all add up to 1. As expected, this leads to reduced success probabilities for the same set of actions under the influence of multiple simultaneous criticalities. In the state transition diagram (Figure 5), it should be noted that if there is a combination of two criticalities ($c1$ and $c3$, or, $c1$ and $c4$) or three criticalities ($c1$, $c3$, and $c4$), it may be possible to take response actions such that all the intermediate states are bypassed. However, this direct transition to the normal state excludes the actions pertaining to $c1$ and focuses only on evacuation of people to temporary refuge.

V. Evaluation of The Crisis Response Process for Fire Emergencies in OGPP

This section presents a simulation based analysis evaluating the performance of the criticality response using CRM model. We simulated the scenario of fire emergency musters on OGPP as described in the previous section. Two different response action selection approaches have been evaluated:

1) *Greedy* approach – selects response actions corresponding to ML with maximum probability (oblivious to the possibility of any subsequent criticalities)
2) *Mitigative Action based Criticality Management (MACM)* approach – selects response actions corresponding to ML with maximum Q-value [4].

For example, the greedy approach selects *RC*3 at state 143 in Figure 5 to transit to state 14, whereas the MACM approach selects *RC*3, and *RA* from state 143 to transit directly to n. This way any intermediate criticalities due to human errors are avoided. The goal of the simulation based evaluation is – i) to

verify the applicability of Q-value as the manageability metric; and ii) to compare the manageability of the fire emergency in OGPP for both greedy and MACM approaches.

A. Simulation Model

The simulator was developed in C++ where the criticalities were implemented as timer events. We implemented the state transition hierarchy in Figure 5 as an adjacency matrix with the values representing the probabilities of state transition. Different experiments, varying the time to perform response actions and to detect criticalities, were performed on the same adjacency matrix for consistency. The probabilities associated with CLs therefore determine the timer triggers that result in the lower-level criticality. The response actions (weights for the MLs) are implemented as timer waits for performing the actions. The criticality detection was performed in a periodic manner. The criticality detection period and the time for the criticality response actions (which depend on the structure and architecture of the OGPP) are varied to observe the response actions' manageability, measured in terms of the Q-value. These experiments were further performed for differing number of simultaneous criticalities.

B. Simulation Results

Figure 6 compares the manageability achieved by the Greedy approach and the MACM approach. The comparison is performed for – i) varying criticality detection delay, ii) different time to perform response action (the results are taken for varying the response action time for criticality c4 only to avoid repetition), and iii) different number of simultaneous criticalities. Results show that the greedy approach may lead to lower manageability. The MACM approach, on the other hand, achieves better manageability. It can be concluded that response actions, oblivious to the subsequent criticalities (as in Greedy approach), result in less manageability even with high immediate success probability. This validates the applicability of the Q-value as the manageability metric.

Increasing the time for criticality response actions has similar effect as increasing the period of detection as both may lead to violation of the controllability condition. The set of results in Figure 7 shows these variations using the MACM approach for different number of simultaneous criticalities. As expected, we find that as period of detection and criticality response actuation time increase, the manageability either remains the same or decreases, drastically in some cases due to controllability condition violation (Figure 7). Further, as expected, the manageability decreases with any increase in number of simultaneous criticalities (Figures 6 and 7). These results further validate the Q-value as the manageability metric.

The actuation delay of response to c4 has higher impact on the manageability (Figures 7(c) and (d)) when compared to the actuation delay of response to c1 (Figures 7(a) and (b)). This is because the response to c4 contributes to more MLs – MLs from states 14, 143, and 134 (Figure 5) – than the response to c1 (ML from state 1). Informally, this means that evaluation of and movement along the evacuation paths should be fast enough to minimize life losses (again validating the applicability of the Q-value as the metric for the manageability of the criticalities).

VI. Conclusions

Criticality Response Modeling (CRM) framework was developed enabling objective evaluation of crises response processes. The evaluation determines the effectiveness of crises response in terms of manageability (measured as the Q-values of the response actions for the criticalities occurred). CRM was applied for fire emergencies in OGPP. As expected, the criticality detection delay and the response actuation delay inversely affects the manageability validating the applicability of Q-value.

The CRM framework can be further used to perform comparative study on the outcome of different response actions. In this regard, CRM was used to compare the manageability of two different response action selection criteria in OGPP. Results showed that response actions, oblivious to the subsequent criticalities, result in less manageability – further validating the applicability of Q-value as the manageability metric.

Also, such comparison and evaluation, enabled by the CRM framework, can incur significantly steeper learning curve for the smart-infrastructure resulting in better crises preparedness – one of the most difficult challenges in homeland security.

Acknowledgements

The authors are thankful to Krishna Venkatasubramanian for his contributions in developing the simulaton model; and to Mediserve Inc., Intel Corp., and the Consortium of Embedded Systems for supporting the research.

References

[1] Computer Science and Telecommunication Board, National Research Council, "Summary of workshop on information technology research for crisis management," The National Academy Press, Washington D.C., 1999.

[2] P. C. Light, "The katrina effect on american preparedness – a report on the lessons americans learned in watching the katrina catastrophe unfold," 2005, available at http://www.nyu.edu/ccpr/katrina-effect.pdf.

[3] F. Adelstein, S. K. S. Gupta, G. G. Richard, and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*. McGraw-Hill, 2004.

[4] T. Mukherjee, K. K. Venkatasubramanian, and S. K. S. Gupta., "Performance modeling of critical event management for ubiquitous computing applications," in *MSWIM*, Spain, 2006.

[5] S. S. Yau, F. Karim, Y. Wang, B. Wang, and S. K. S. Gupta, "Reconfigurable context-sensitive middleware for pervasive computing," in *IEEE Pervasive Computing, joint special issue with IEEE Personal Communications on Context-Aware Pervasive Computing*. Los Alamitos, USA: IEEE Computer Society Press, 2002, pp. 33–40.

[6] S. Mehrotra *et al.*, "Project RESCUE: challenges in responding to the unexpected."

[7] D. Mosse *et al.*, "Secure-citi critical information-technology infrastructure."

[8] U. Gupta and N. Ranganathan., "Firm: A game theory based multi-crisis management system for urban environments," in *Intl. Conf. on Sharing Solutions for Emergencies and Hazardous Environments*, 2006.

[9] K. M. Chandy *et al.*, "www.infospheres.caltech.edu/," caltech Infosheres Project.

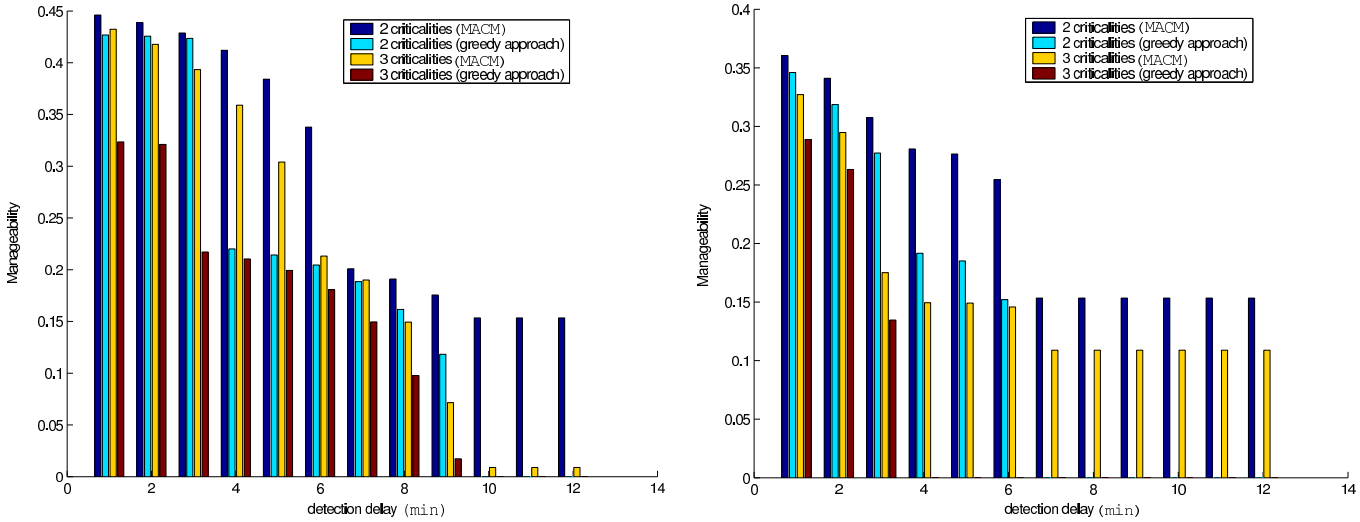
[10] K. M. Chandy, "Sense and respond systems." in *31st Int. Computer Management Group Conference (CMG)*, Dec 2005.

[11] N. Leveson, *Safeware: System Safety and Computers*. Addison Wesley, 1995.

[12] J. C. Knight, "Safety-critical systems: Challenges and directions," in *Proceedings of ICSE'02*, Orlando, Florida, Jul 2002.

[13] S. K. S. Gupta, T. Mukherjee, and K. K. Venkatasubramanian., "Criticality aware access control model for pervasive applications." in *IEEE PerCom*. IEEE, 2006, pp. 251–257.

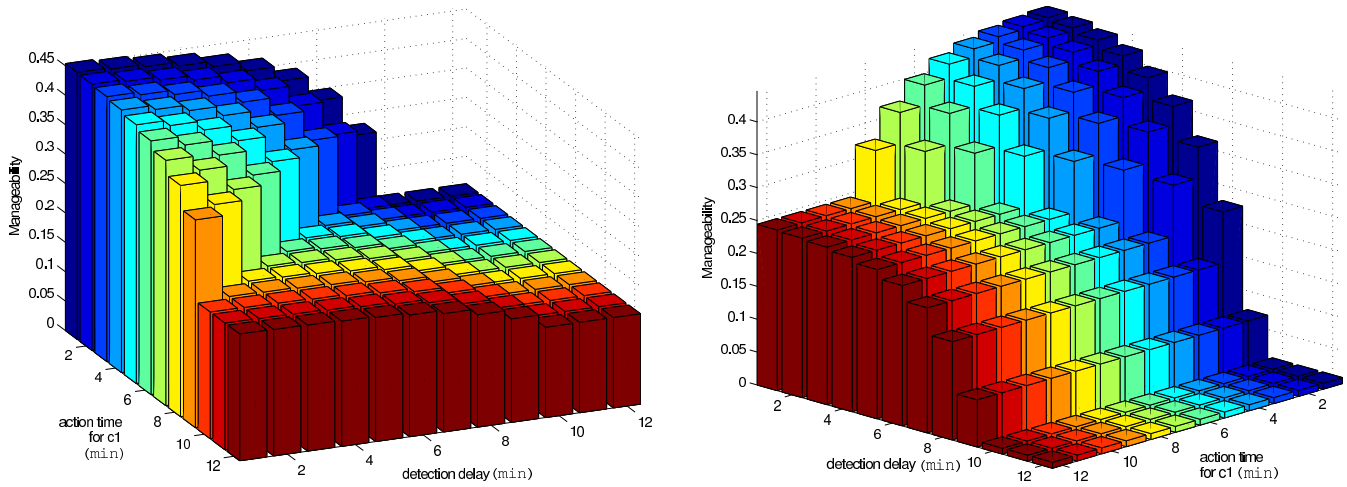
[14] D. G. DiMattia, F. I. Khan, and P. R. Amyotte, "Determination of human error probabilities for offshore platform musters," *Journal of Loss Prevention in the Process Industries*, vol. 18, pp. 488–501, 2005.



(a) $c4$ action time = 1 minute

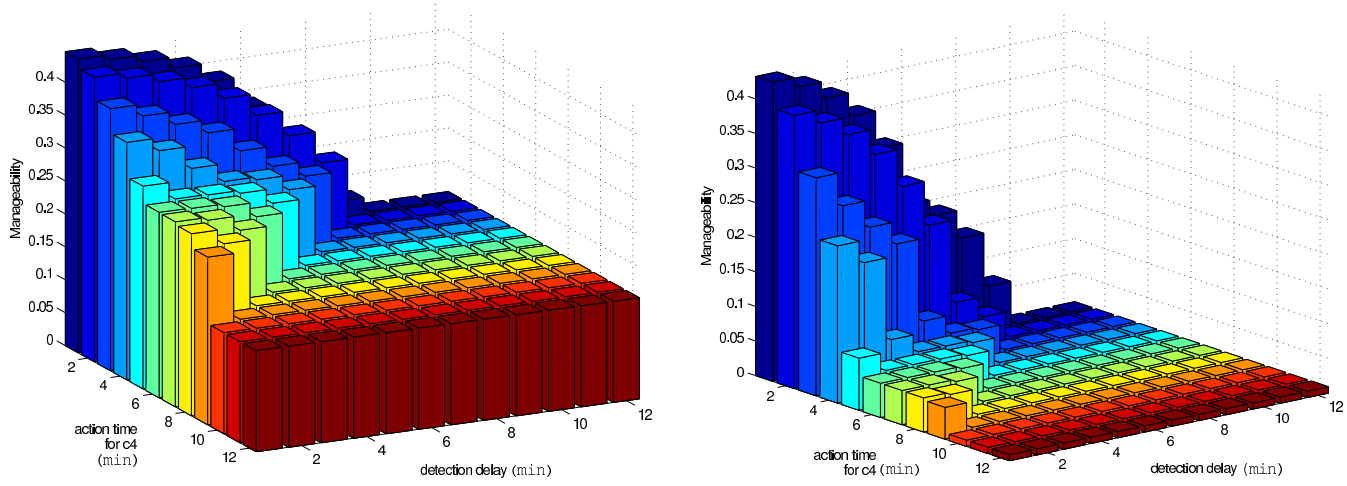
(b) $c4$ action time = 4 minutes

Fig. 6. Variation of manageability for response actions selected by Greedy and MACM approach (w.r.t. detection delay and actuation delay in response to $c4$).



(a) 2 simultaneous criticalities

(b) 3 simultaneous criticalities



(c) 2 simultaneous criticalities

(d) 3 simultaneous criticalities

Fig. 7. Variation of manageability using MACM approach w.r.t. detection delay and action time for responding to $c1$ and $c4$.