Advanced Science and Technology Letters
Vol.52 (AICT 2014), pp.42-55
http://dx.doi.org/10.14257/astl.2014.52.08

Emergency Management System Requirements Definitions of Safety-Critical System Using The Behavioral Patterns Analysis (BPA) Approach

Dr. Assem El-Ansary, CEO

Emergent Technologies USA, Inc.
assem_elansary@yahoo.com

Abstract. This paper illustrates the event-oriented Behavioral Pattern Analysis (BPA) modeling approach in developing an Emergency Management System (EMS). The Event defined in BPA is a real-life conceptual entity that is unrelated to any implementation. The major contributions of this research are: the Behavioral Pattern Analysis (BPA) modeling methodology, and the development of an interactive software tool (DECISION), which is based on a combination of the Analytic Hierarchy Process (AHP) and the ELECTRE Multi-Criteria Decision Making (MCDM) methods.

Keywords: Analysis, Emergency Management System, Safety-Critical System, modeling methodology, software modeling, event-oriented, behavioral pattern, use cases

1 Introduction

Experience reports problems with Use Cases such as [1] lack of a formal specification, lack of atomicity which has made the measurement of a project's task complicated, and a problem with the phrase use case itself.

A major problem in the use case approach is its tendency to focus on the solution rather than the problem. Jacobson defined use case as “a behaviorally related sequence of transactions in a dialogue with the system” [2]. The processing of transactions, or operations, or use cases is what the machine does. It is part of the solution, not part of the problem [3].

The concluding statement of the “Question Time! About Use Cases” Panel of the OOPSLA'98 Conference by Ian Graham [4] was “There is a need for another modeling methodology with a sound theoretical basis and a precise definition.” This need is what this research is about.

In addition to the problems with the use cases [3][4] that were described briefly above, several additional problems were identified during this research [5], [6]. The following is a discussion of these problems:

- The types of interactions are: interactions among users, interactions between users and the system, and interactions among the different components of the system. Yet, use cases describe only the users' interaction with the system.

ISSN: 2287-1233 ASTL

 Using natural language in use cases description, with the absence of any semantic structure such as alternation or repetition, increases the risks of ambiguity, incompleteness, and inconsistency.

In conclusion, if the analyst misinterpreted or neglected some structural or behavioral aspects, the resulting conceptual model will not be a good representation or understanding of the real world. The resulting software solution system built from the model may not demonstrate the correct behavior or may ungracefully terminate. The end result might be the loss of opportunities in using business systems, serious damages in embedded systems, or the loss of lives in using a safety-critical system.

In the BPA modeling methodology, the BPA Behavioral Pattern, which is the template that one uses to model and describe an event, takes the place of the Use Case in the UML Use Case View. The BPA Behavioral Patterns are temporally ordered according to the sequence of the real world events.

2 Illustrating BPA through the Emergency Management System (Ems)

Workplace Emergency is an unforeseen situation that threatens employees, customers, or the public, disrupts or shuts down operations, or causes physical or environmental damage.

The types of Emergency Management System (EMS) [7] are: Earthquakes, Hurricanes, Tornadoes, Energy/utility, outages, Fire hazards, Hazardous materials releases, Terrorism.

Phases of Disaster Preparedness are: Prevention – Mitigation, Planning, Response / Preparedness, Recovery.

 National Incident Management System (NIMS) was established by Presidential Directive (HSPD 5) in February 2003 to create a national comprehensive system for the management of domestic emergencies.

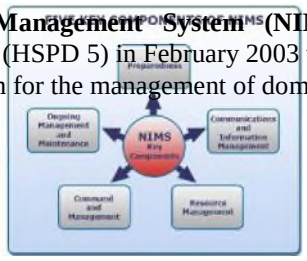


Fig. 1 NIMS Key Components

2.1 Mitigation and prevention

These are actions aimed at reducing or eliminating the impact of future hazard events by avoiding hazard or strengthening resistance to it.
Mitigation Program is shown in Fig. 5.

2.2 Emergency Preparedness

Essential elements of emergency preparedness are:

- Identify hazards and assess risk.
- Develop an emergency plan and procedures.
- Integrate the plan with the community plan.
- Conduct training.
- Public relations.
- Conduct Drills and Exercises.
- Develop Plan Audit Procedures.

2.3 Emergency Response

OSHA"s Response to Emergency is:

- To assist local response agencies in any way possible within agency capabilities (Non-enforcement)
- To initiate workplace investigation (Enforcement)
  What is the Response Phase?
- Response is taking action to effectively contain and resolve an emergency
- Steps taken during this phase to implement the emergency management plan include:
  - Activating the plan
  - Deploying resources
  - Activating communication plans
  - Working with community partners/first responders
  - Accounting for students and staff
  - Making informed decisions
  - Accelerating the Recovery phase

  Response Key Components are shown in Fig. 8.

2.4 Emergency Recovery

Why Recovery?

- Decreasing natural vulnerability
- Decreasing human vulnerability
- "Fragile" states unable to address disaster situations = greater tragedy

Recovery key components are shown in Fig. 9.

3 The BPA Requirements Development Procedure

The following is an outline of the BPA functional requirements development procedure (Fig. 8 and Fig 9):

1. Identify the problem at the highest level of abstraction (e.g. The Mission Statement and Operating Requirements).
2. Identify the scope of the requirements (problem) from the Originating Requirements.
3. Analyze the Originating Requirements to identify the Critical Constraints (e.g. Safety) and/or the Utility Requirements.
4. Decompose the scoped problem (from step2) into Main Events based on the Mission and Operating Requirements (Step I).
5. Using the identified Main Events, draw the High Level Event Hierarchy Diagram which is constructed in several levels whose top level includes the highest main event (Fig. 10).
6. Decompose these identified Main Events into smaller and simpler events represented as Episodes (Composite Events) with clear boundaries[1].
   - An Episode Boundary at this stage may be marked with Location / Loci of Control and Effect.
7. Add additional levels to the Event Hierarchy Diagram (Event Hierarchy Sub-Diagrams) Fig. 11, 12, 13, 14, and 15. For complex problems, it is often helpful to extract these sub-diagrams and analyze them. Detailed level event hierarchy diagrams are drawn as necessary.
   - Decomposition Heuristics at this stage is ' One Agent and One Location'
8. For each identified main event (from step 4) draw an Event Thread Diagram which represents the events' sequence (Fig. 16)
   - Starting with the Main Events, as initial composite events, recursively decompose the composite events into Basic Events
   - The Event Decomposition Heuristics at this stage is ' One Agent, One Location, One Motion Direction, and One Time Interval'.
   - Group Basic Events by their Location / Loci of Control and Effect. Draw a frame box around these Basic Events
9. Refine and transform the above Basic Events into their corresponding BPA Behavioral Patterns which describes the which, who, when, and where of each of the basic events (Fig. 5)
10. Using the Event Thread Diagrams from step 8, draw the Temporal/Causal Constraint Diagrams by adding the temporal constraints (time order as illustrated in Fig. 6 and Fig 7) alongside the associations and identifying the enable/causal relationships (Enable is what makes it ready, and Causal means making something happen) in each corresponding Event Thread Diagram (Fig. 8).
11. Using the Critical Constraints (e.g. Safety), identify the critical events, identify all possible ways of each critical event's failure, and draw the Critical Event Analysis Diagram (Fig. 9).
12. Using the BPA Event Patterns and the Critical Event Analysis Diagrams, identify any missing requirements that are necessary to satisfy the critical

constraints. One develops a Derived Requirements document and get users approval on this document.

13. Using the Missing Requirements (from step 12), refine the Event Hierarchy Diagram (from step 6), the Thread Diagrams (from step 8), and the Temporal Constraint Diagram (from step 10) as necessary. Draw additional Event Thread Diagrams for identified critical events as necessary.

    The figure below illustrates the BPA iterative and incremental development process. The figure shows the start with the Originating Requirement and Steps 1 to 3, then Steps 4 to 7, then Step 8, then Refine and come-up with the Derived Requirements which covers any Missing Requirements as explained in Steps 9 and 10. After that we re-iterate as explained in Steps 11 and 12.

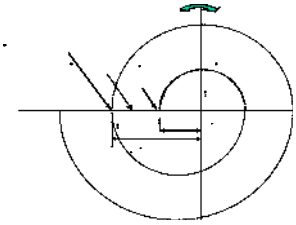


Fig. 2 The BPA Modeling Process

14. Using the BPA Behavioral Patterns (from step 9), identify the candidate Classes from the Event Roles (Participants) and Instrument. Draw the Class Diagram (Fig.10).
15. To illustrate the relationship between Events and States, optionally, using the BPA Behavioral Patterns, draw the Event/State History Chart (Optional – not shown) that includes the States before and after each Event for each identified Class whose instance is a participant in that Event.

The above procedure illustrates the BPA functional requirements development procedure. Fig. 3 depicts the flow of the modeling activities (Steps 1 to 14) for the BPA procedure.

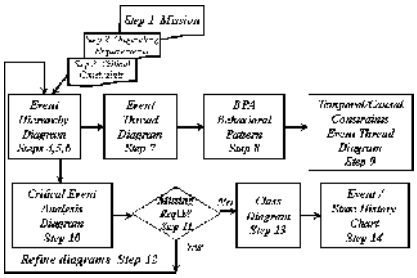


Fig. 3. Requirements Development Procedure

3.1 Event Hierarchy Diagram (EHD)

Event Hierarchy (Fig. 4) is used to model the events at different levels of abstraction (event decomposition). A general problem with decomposition is when to stop the decomposition. T**he decomposition heuristic** used in an Event Hierarchy Diagram (EHD) is one agent and one location. Using this heuristic, a leaf event is usually a set of Basic Events (atomic events) sequenced into episode[1] . The episode is marked with a location boundary. The following is the ITS detailed Event Hierarchy Diagram:

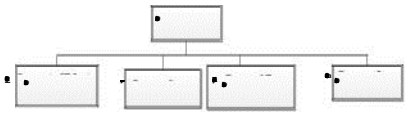


Fig. 4. Event Hierarchy – Emergency Management System (EMS) Planning Phases

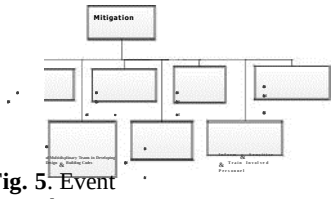


Fig. 5. Event Hierarchy – Emergency Management System (EMS) Mitigation

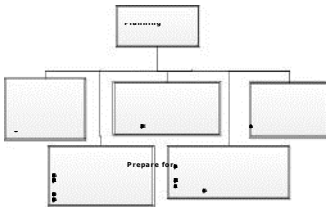
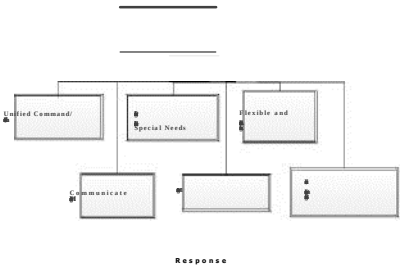


Fig. 6. Event Hierarchy – (EMS)



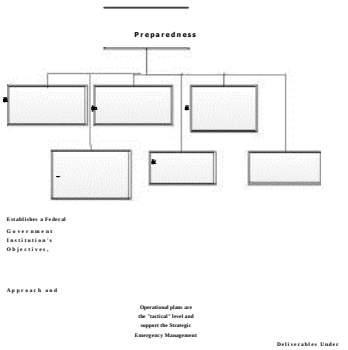


Fig. 7. Event Hierarchy – Emergency Management System (EMS) Preparedness

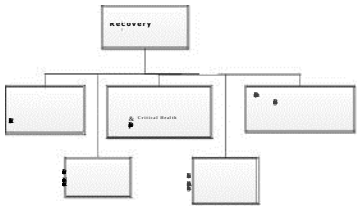
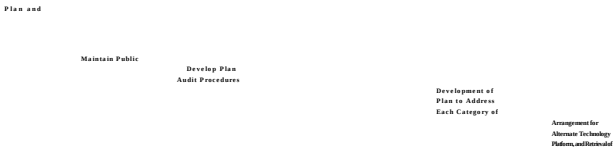


Fig. 8. Event Hierarchy – (EMS) Response

Fig. 9. Event Hierarchy – (EMS) Recovery



Using the identified main events, the high level EHD diagram (or the first level in a detailed EHD diagram) is drawn. Each main event is then decomposed further until one arrives at leaf events, each of which has one location or one locus of effect and control and one agent.

In order to model the sequence of events (and show the location / loci of control and effect view, or the temporal / causal constraints), one uses the event thread diagrams as shown in the next subsections.

3.2 Event Thread Diagram (ETD)

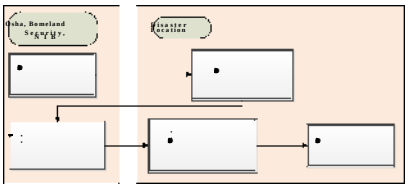


Fig. 10. Event Thread Diagram for EMS

As explained in step 8, the research goal is to develop a requirements definition mechanism (BPA Pattern – Fig. 11) that describes the What, Who, How, When, Where and Why.

3.3 Behavioral Patterns

BPA BEHAVIORAL PATTERN - EXAMPLE

Event (WHAT?) ***Emergency Preparedness***

Prepare for

Prevent _ Mitigate

Respond To

Recover from

1. Identify Hazards &Assess Risk *2. Develop Emergency Plan*
3. Integrate Plan with Community Plan 4. Maintain Public Relations
5. Conduct Training Drills & Exercises *6. Develop Plan Audit Procedures*
Agent a: Chief Emergency
- *Initial State: Identify Hazards and Assess Risk*
- *Final State: Develop Emergency Plan*

Affected p: Incident Location
- *Initial State: Uninformed*
- *Final State: Informed with Emergency Plan*

Modality (HOW?)
Instrument
i: Reports and Communications
Circumstances

Manner
m: Critical
Condition
c1: Released c2:
Effect
f1: Prepared f1:
Date/Time (WHEN?)
t: Before Incident Occurs
Place (WHERE?)
Location
l: Incident Location
Path
Motion
m: N/A
Direction
d: N/A
Rationale (WHY?)
Goal ***g: Develop Emergency Plan and Procedures***
Mental State ***bdi:***
Caused-By *e': Incident*
End;

Fig. 11. BPA Pattern – EMS Preparedness

3.4 Introducing Time

The key intuitions motivating the introduction of time are:

- Events take time. Yet, in most of the popular Object-Oriented Modeling methodologies such as OMT and UML, time is neglected in the event definition.
- Multiple events may occur at the same time, and could be unrelated, cooperating, or interfering with each other.
- Events may have temporal constraints. They may overlap, start or finish together, occur together, or disable (disjoint) each other. BPA uses the time intervals" relations that are described in the Interval Algebra framework [8] to model the temporal relationships between events. In this Interval Algebra framework, seven basic relations can hold between time intervals. Fig. 12 and Fig. 13 illustrates these basic relations for arbitrary events x and y.
- Fig.13 illustrates the Interval Algebra Relations.

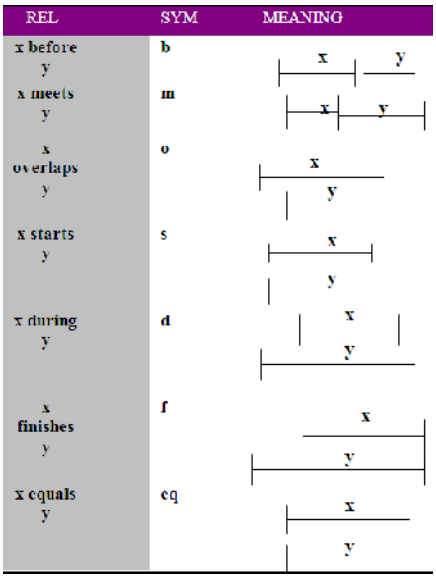


Fig. 12. Time Interval Algebra – Temporal Relations

3.5 Introducing Enable / Cause Relationships

The introduction of the Enable[10] / Cause relationships between events will enable the analyst to do cause effect analysis and reason about any possible failure of the system.

10 -Enable" is defined in the American Heritage Dictionary as: "..To supply with the means, knowledge, or opportunity; make able: *a hole in the fence that enabled us to watch; techniques that enable surgeons to open and repair the heart."*

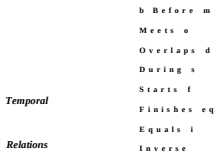


Fig. 13. Time Interval Algebra - Temporal Relations Notation

In the Temporal Constraint Diag., as described in steps 9, and 10, the temporal relations (Fig. 12) are written alongside the sequence relationships to represent the possible timing at which these events can occur.

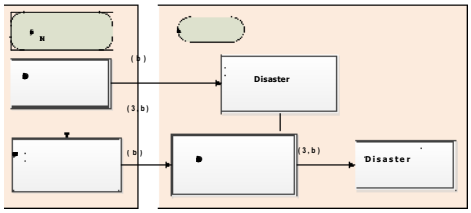


Fig. 14. Temporal Constraint Diagram – EMC

3.6 Failure Issues

Osha, Homeland

Disaster

Prepare for

Prevent _ Mitigate

Respond To

Recover from

The following is a list of reasons of possible failures in responding to events:

> Occurrence of a relevant event which the system does not handle
> Event rate exceeding the system‟s capacity
> Unsuccessful detection and acquisition of all events including manually captured events
> Non-capturing of all information triggered by event
> Failure across man-machine interface
> Failure of Software, Hardware, or Human.

The ability to provide requirements specification for safe behavior is very limited using the current modeling methodologies. Neither a safety analysis (anterior analysis) nor accident analysis (posterior analysis) can be achieved efficiently without event analysis. As will be explained below, the BPA modeling methodology provides the Critical Event Analysis (defined below) as an efficient solution to this problem.

4 Missing Requirements

There were no missing requirements that required generating a Derived Requirement Document.

5 EMS Class Diagram

The resulting Class Diagram is shown in Fig. 22.

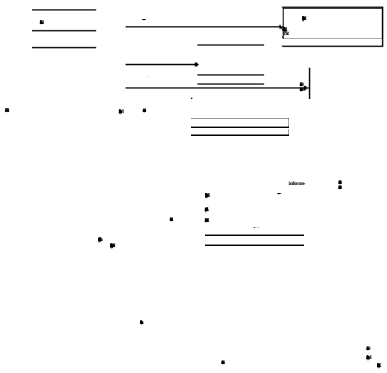


Fig. 15. Class Diagram – EMS Mitigation

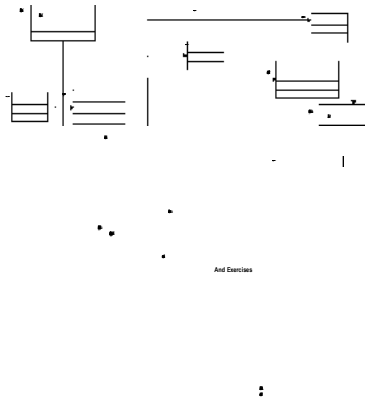


Fig.17. Class Diagram – EMS Preparedness

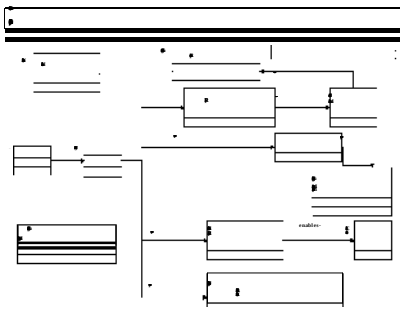


Fig. 16. Class Diagram – EMS Planning

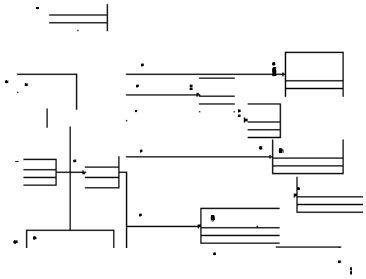


Fig. 18. Class Diagram – EMS Recovery

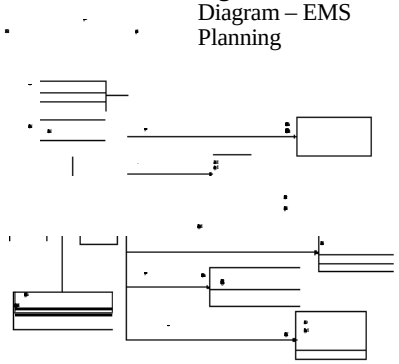


Fig. 19. Class Diagram – EMS Response

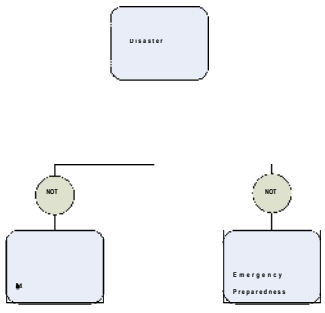


Fig. 20. Critical Analysis Diagram – EMS

Analysis procedure includes the following steps:

6.1 Critical Events Analysis

The requirements should correctly reflect the critical properties of the environment in which software is to work. In order to gain as much confidence as possible in the software for a critical system, the analyst should perform a "Critical Event Analysis". The Critical Event

Emergency

- Identify Critical Events
- For each critical event, identify all possible ways in which it may fail
- Capture these possible failure modes using the undesired event notation
- Study each undesired related state to find out how to achieve protection against such possible failure.

7 Evaluation of the Effectiveness of BPA and UCA

7.1 The Effectiveness Metrics

The effectiveness metrics categories used in this research include:

1. System Effectiveness represented by safety
2. Requirements Engineering Process Effectiveness represented by the CMM [12] and CMMI repeatability
3. Definition of Requirements Effectiveness represented by the ANSI (NIST) / IEEE Std 830-1984 [13] for systems specifications such as Unambiguity, Completeness, Consistency, Modifiability, and Traceability.

8 The Pairwise Comparison Method

A Multi-Criteria Decision Making (MCDM) Tool, named as DECISION, was developed by this researcher to evaluate the assessment results. The Decision tool uses a combination of the Analytic Hierarchy Process (AHP) and the ELECTRE Pairwise Comparison approaches. Pairwise Comparisons is the process in which experts rate a set of objects, events, or criteria, by comparing only two at a time [14]. The selected approaches, AHP and ELECTRE, are popular and have strong theoretical basis [15], [16].

9 The Case Study Material

Each SME was given a case study kit that contains the instructions, an application, an overview and a step by step procedure describing how to analyze and model requirements using the UCA and BPA modeling methodologies, two analyses of the given application; one using UCA and the other using BPA, explanation of the Pairwise Comparison and the effectiveness criteria, and Evaluation Forms.

10 The Subject Matter Experts

The number of SMEs depends on the number of the controlled variables. The controlled variables are:

- The applications.
- The set of the SMEs.
- The SMEs‟ software engineering experience:
  - Structured Analysis
  - Use Case Analysis / UML.

11 CASE Studies' Results

11.1 Case Studies Results

11.1.1 AHP Results

Results in Fig. 21 gives 93.8 % approval rate for the thesis hypothesis with about three times overall effectiveness for BPA over UCA.

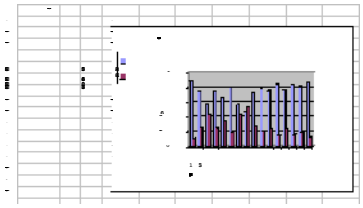


Fig. 21. Effectiveness Evaluation of BPA versus UCA – Results using AHP

11.1.2 ELECTRE Results

Fig. 22. ELECTRE Evaluation Results‟ Summary

Fig. 22 shows that there is 87% approval rate for the thesis hypothesis.

12 Why This Work Is Important

12.1 Real-time Systems

In most of the popular object-oriented development modeling methodologies state diagrams are used to model the behavior. State diagrams are focusing on an individual object's response to specific events rather than objects interaction. By describing the requirements in terms of events, represented by the behavioral patterns, all of the object's interactions are considered.

13.2 Multi-agent Systems

There is a need for a multi-agent systems analysis and design method that is powerful enough to model interaction patterns involving autonomous agents.

13.3 Safety-critical Systems

In these systems, analysts should perform a "Safety Analysis'. Using BPA, one identifies and documents the critical events during the requirements definition stage.

GOD says [KORAN][TORAH], " ... Whoever rescues a single life earns as much merit as though he had rescued the entire world." If the use of the BPA Modeling methodology may save one life, the significance of this modeling methodology is immeasurable.

References

1. Graham, I.: Migrating to Object Technology, Addison-Wesley, Reading, Massachusetts, 1995.
2. Jacobson, I., Christeron, M., and Overgaard: Object-Oriented Software Engineering: A Use Case Driven Approach, Addison-Wesley, Massachusetts, 1992.
3. Jackson, M.: Software Requirements & Specification, A Lexicon of Practice, Principles and Prejudices, ACM Press, Addison-Wesley, Reading, Massachusetts, 1995.
4. Martin, F., and Cockburn: Question Time! About Use Cases, OOPSLA'98 Proceedings, ACM Press, New York, NY, 1998.
5. El-Ansary, Assem I.: Behavioral Pattern Analysis: Towards a New Representation of Systems Requirements Based on Actions and Events, in Proceedings of the 2002 ACM Symposium on Applied Computing, ACM, New York, NY, 2002.
6. El-Ansary, Assem I.: Behavioral Pattern Analysis: Towards a New Representation of Systems Requirements Based on Actions and Events, Doctoral Thesis, George Mason University, 2005.
7. Carpens, J., A, etal.: Emergency Response, OSHA, 2005 Swiri Annual Meeting, 2005.
8. An Overview of the Four Phases of Emergency Management for Schools, U.S. Department of Education Office of Safe and Healthy Students (OSHS) Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center.
9. NIH Emergency Management/Continuity of Operations Program Overview Briefing.
10. Clerk, Ed and Moffett, Emergency Management for Schools training, Philadelphia, PA, 2007

11. Allen, J. F., Maintaining Knowledge about Temporal Intervals, Communications of ACM, 26, 1983, pp 832-843
12. Leveson, N.: Safeware, Addison-Wesley, Reading, Massachusetts, 1995.
13. Lewerentz, C., and Lindner, T.: Formal Development of Reactive Systems, Springer-Verlag, NY, 1995.
14. Heitmeyer, Constance and Mandrioli, Dino, Formal Methods for Real-Time Computing: An Overview, in Formal Methods for Real-Time Computing, John Wiley & Sons, Inc., NY, 1996.
15. Humphrey, W.: Software Process Maturity Framework, Addison-Wesley, MA, 1989.
16. IEEE and ANSI, ANSI/IEEE Std 830-1984, IEEE Guide to Software Requirements Specification, in System and Software Requirements Engineering, IEEE Computer Society Press, Los Alamitos, California, 1990, pp 170-192.
17. Saaty, Thomas L.: Decision Making for Leaders, Wadsworth, Inc., 1982.
18. Meyer, M., and Booker, J.: Knowledge Based Systems Vol. 5, Eliciting and Analyzing Expert Judgment, A Practical Guide, Academic Press, 1991.
19. Bui, Tung X.: Co-oP, A Group Decision Support System for Cooperative Multiple Criteria Group Decision Making, Springer-Verlag, 1987.

