U.S. Department of Homeland Security
Advanced Scientific Computing Program

Computer Simulation for Emergency Incident Management

Report of the Department of Homeland Security Incident Management Simulation Workshop

Washington D.C.

May 12-13, 2004

Department of Homeland Security Advanced Scientific Computing Program

UCRL-CONF-208718
Lawrence Livermore National Laboratory
University of California Livermore, California 94550

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

EXECUTIVE SUMMARY

Since the dawn of the age of electronic computers, their potential value in assisting with training and education has been clear. By the 1960's, instructional materials that included simple computer-graded evaluation tests started to appear. As computational power increased, computer-based training became more sophisticated, particularly as graphical displays and processor speed developed to the point that visual realism became possible. By the 1990's, particularly in the U.S. defense sector and in the aviation industry, computer-driven training systems that included full immersive environments were deployed. While these systems were quite expensive, they allowed for considerable cost savings in some aspects of training; an important example is the training simulators used to train airplane and helicopter pilots. In recent years, processor speed has increased, and cost has decreased to the point that realistic visual simulations are available as part of game boxes priced well within the realm of the average consumer. For example, ***Full Spectrum Warrior™***[1] for the Xbox™ game station, is billed as a "realistic portrayal of Infantry-level urban warfare … commissioned by the U.S. Army". At the high-end, full virtual reality training environments with optical, aural, and tactical stimulation are under development, particular in the DoD community, where the vision for a fully immersive training environment is likely to be realized within this decade.

In the homeland security realm, the potential value of realistic computer simulation for training purposes is clear. Incident-response professionals can increase their proficiency in managing catastrophic events if they train against catastrophic situations that stress their capabilities. Immersion-based simulation technologies can create "real-world" environments capable of challenging decision making skills and accurately presenting the down-stream consequences of those decisions. Since many professionals will never encounter a truly catastrophic event, simulations can be used to prepare those professionals to meet the demands of these events. In particular, such simulations can be used to help assess and improve response plans for catastrophic events. Unlike current training exercises such as TOPOFF, a computer-based simulation does not have to be scripted. Instead, the computer creates an environment that represents the dynamic behavior of the physical environment as events occur and people respond. Since actions of the players in the simulation change the sequence of events, a given event can be simulated multiple times, and the consequences of different incident-management choices can, therefore, be evaluated.

Because of the complexity, sophistication, and realism of the simulation tools that will be required for training purposes, a reasonable question to ask is if such tools could be used during an actual event as predictive tools to aid in the decision-making process as an event unfolds. While this concept

[1] http://www.xbox.com/en-us/fullspectrumwarrior/

seems clear, the software development requirements for tools that would be required to operate reliably during a crisis would be significantly more stringent and, therefore, more expensive than those required to develop training software. This report includes a discussion of simulation technologies that could be applied in real event decision making situations, but the recommendations of this report are limited to the application of computer simulation to incident-management training.

Another issue is the use of computer software for the purpose of evaluating performance, either during training or during an actual incident. Unlike the early training tools described above, large-scale simulation tools, such as those envisioned here, should probably not be used for automatic (i.e. computer-driven) evaluation of incident-management performance. Because of the lack of foreknowledge and the complexity of these events, replacing expert human evaluation with automatic evaluation of performance would be technologically very difficult and probably not warranted. It is well recognized that expert human judgment should be applied to the evaluation of the success and quality of response by those being trained. However, a properly implemented simulation system could be very helpful in gathering metrics and patterns of communication and other behavior, difficult or impossible to gather during an actual incident response, that would support and objectify expert human judgment.

From a technological perspective, computer-simulation tools that will allow professionals to train for highly complex and unexpected homeland security events will themselves be highly complex. All aspects of physical infrastructure must be modeled in addition to the behavior of the population in response to an unfolding event. Each of these aspects will be modeled separately and must be coupled together effectively in order to represent the complete reality. While current technology can be adapted to provide some level of catastrophic incident training facility, there are research and development issues that must be addressed in order to provide high-fidelity simulations that are desirable for fully effective incident management training.

This report describes the findings and recommendations resulting from the DHS Incident Management Simulation Workshop held by the DHS Advanced Scientific Computing Program in May 2004. This workshop brought senior representatives of the emergency response and incident-management communities together with modeling and simulation technologists from Department of Energy laboratories. The workshop provided an opportunity for incident responders to describe the nature and substance of the primary personnel roles in an incident response, to identify current and anticipated roles of modeling and simulation in support of incident response, and to begin a dialog between the incident response and simulation technology communities that will guide and inform planned modeling and simulation development for incident response. This report provides a summary of the discussions at the workshop as well as a summary of simulation capabilities that are relevant to incident-management training, and

recommendations for the use of simulation in both incident management and in incident management training, based on the discussions at the workshop. In addition, the report discusses areas where further research and development will be required to support future needs in this area.

Report Authors

David Brown, Lawrence Livermore National Laboratory
Budhendra Bhaduri, Oak Ridge National Laboratory
Celeste Matarazzo, Lawrence Livermore National Laboratory
Mike Mercer, Lawrence Livermore National Laboratory
John Shadid, Sandia National Laboratories
Robert Hills, Lawrence Livermore National Laboratory
Jon Sorensen, Oak Ridge National Laboratory
Douglas Speck, Lawrence Livermore National Laboratory
Brian Worley, Oak Ridge National Laboratory

Acronyms and Abbreviations

AAR	After Action Review
ASC	Advanced Scientific Computing (Program, DHS S&T)
CBRN	Chemical-Biological-Radiological-Nuclear
CNN	Cable News Network
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
EEI	Essential Elements of Information
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EP&R	Emergency Preparedness and Response
ER	Emergency Responder
ESF	Emergency Support System
FBI	(U.S.) Federal Bureau of Investigation
FDNY	Fire Department of New York
FEMA	Federal Emergency Management Agency
GIS	Geographical Information System(s)
HAZMAT	Hazardous materials
HAZUS	Hazards US (FEMA loss estimation software system)
HLA	High Level Architecture (framework for software development)
HVAC	Heating, Ventilating, and Air Conditioning
IC	Incident Commander
ICS	Incident Command System
IMS	Incident Management Simulation
LEPC	Local Emergency Planning Committees
MS&G	Modeling, Simulation and Games
NIMS	National Incident Management System
NYPD	New York Police Department
ODE	Ordinary Differential Equation
ODP	(DHS) Office of Domestic Preparedness
PDE	Partial Differential Equation
PFD	Phoenix Fire Department
PIO	Public Information Officer
RACES	Radio Amateur Civil Emergency Service
REACT	Radio Emergency Associated Communications Teams
R&D	Research and Development
SEMS	(California) Standardized Emergency Management System
SOC	State Operations Center
S&T	Science and Technology (Directorate, DHS)
TOPOFF	Top Officials (WMD response exercise)
UC	Unified Command
USFA	US Fire Administration
USGS	US Geological Survey
WMD	Weapons of Mass Destruction

Chapter 1. The Incident Management Simulation Workshop

The Department of Homeland Security (DHS) Incident Management Simulation (IMS) Workshop was held on May 12, 2004 at the Westin Grand Hotel in Washington, DC. The workshop brought together senior representatives of the emergency response and incident management communities with modeling and simulation technologists from Department of Energy (DOE) laboratories. The goals of the workshop were to provide an opportunity for incident responders to describe the nature and substance of the primary personnel roles in an incident response, to identify current and anticipated roles of modeling and simulation in support of incident response, and to begin a dialog between the incident response and simulation technology communities that will guide and inform planned modeling and simulation development for incident response.

The workshop was a joint effort of the Advanced Scientific Computing (ASC) Program and the Emergency Preparedness and Response (EP&R) Portfolio, both elements of the DHS Science and Technology Directorate. The impetus for the workshop began with a presentation made by Dave Garratt of FEMA at the ASC Requirements Workshop in October, 2003[2]. In his presentation, "NIMCity A National Incident Management Virtual Environment Concept Overview,"[3] Mr. Garratt articulated a vision for a scalable and configurable simulation environment that could simulate any foreseeable event, on any relevant scale, and let incident-response leaders experience the impacts of their decisions in real-time. In this vision, a "NIMCity" would objectively reveal the effects of good and bad communication, good and bad cooperation, and good and bad decisions. It would encourage communities to contribute to a national repository of electronic infrastructure descriptions, and it would permit test and evaluation of new response procedures and technology innovations.

Mr. Garratt's presentation energized many who heard it with the vision of an application that could leverage modern computing power to benefit a critical sector of the nation's homeland security workforce and make a material contribution to our ability to endure the kind of catastrophic scenarios that 9/11 presages. This application encompasses notable research challenges yet is in significant ways realizable with existing state-of-the-art technology and effective system engineering.

Many current models exist that simulate specific physical and behavioral processes necessary for NIMCity to realize its potential. There are also existing examples of higher level agent-based simulations for training and

[2] U.S. Department of Homeland Security Advanced Scientific Computing Program Requirements Worskhop Report, Lawrence Livermore National Laboratory Report UCRL-AR-202297, February 2004.

[3] Mr. Garratt's presentation can be found at the ASC Program Requirements Workshop website at http://www.ascworkshop.info/ .

tactical analysis that might be classified functionally as precursors of NIMCity. Originating in the U.S. Department of Defense (DoD), DOE, academic, and commercial environments, these applications and supporting developments, such as DoD's High Level Architecture (HLA) for simulation reuse and interoperability, contain a wealth of applicable knowledge and accumulated wisdom. Any serious effort to develop NIMCity must begin by mining existing approaches to benefit from the experience they offer. While doing so, it should be recognized that these applications were not designed to provide the comprehensiveness and scalability proposed for NIMCity and will inevitably harbor constraints that, if incorporated into the NIMCity framework, will impede realization of NIMCity's goals.

Keeping NIMCity development on track and avoiding the design and performance limitations of its precursors requires starting with a comprehensive requirements definition and routine iteration during its development with end users in the incident-response community. The IMS Workshop provided an important beginning for these activities. The workshop gave a collection of senior representatives of the emergency-response and incident-management communities, who between them brought literally hundreds of person-years of relevant experience to the workshop, the opportunity to sketch a basic picture of roles and issues in incident response and provide a review of how simulations are used and perceived today. The workshop also paved the way for establishing relationships between a motivated, informed assembly of incident responders, modeling and simulation technologists, and DHS program managers. These relationships will be crucial to ensure appropriate bilateral communication between end users and developers as NIMCity takes shape.

This workshop report is divided into six chapters:

- Chapter 1. The Incident Management Simulation Workshop
- Chapter 2. Morning and Afternoon Sessions Summaries–this is a summary of the ideas and observations articulated during the Workshop. This chapter is divided into two sections following the format of the Workshop, i.e., one session was devoted to emergency response, and one session was devoted to incident management.
- Chapter 3. An Overview of the Role of Simulation in Incident Management – this chapter provides a supporting foundation of knowledge about modeling and simulation, especially in the context of incident response.
- Chapter 4. Simulation Usage and Needs – this chapter elaborates on the ideas revealed during the workshop from the informed perspective of simulation technology developers with experience in agent-based, man-in-the-loop technologies and develops specific recommendations for simulation software development in support of incident-management training.
- Chapter 5. Research and Development Requirements for Advanced Simulation in support of Incident Management – this chapter briefly discusses a number of areas for technology research and development relevant to NIMCity.
- Chapter 6. Conclusions

Chapter 2. Morning and Afternoon Session Summaries

During the workshop on May 12, 2004, two groups of incident-management professionals met with representatives of the DOE Simulation Technology community in four separate hour-long, moderated discussions. These discussions provided an opportunity for the incident responders to describe the nature and substance of the primary personnel roles in an incident response, to identify current and anticipated roles of modeling and simulation in support of incident response, and to begin a dialog between the incident-response and simulation-technology communities aimed at guiding and informing the development of computer-based modeling and simulation tools for incident-response training.

The information below consists of the observations and commentary provided by response community Workshop participants, organized by topic. Although both sessions were motivated by the same basic questions, discussions evolved organically and the resultant topic categories for each session are similar but not identical. Note also that the information in each category is not necessarily comprehensive. In particular, neither session explored the National Incident Management System (NIMS), recently released by the federal government. NIMS supersedes and incorporates the Incident Command System (ICS) and must now be considered a basic feature of the incident response landscape. However, it is too new to have had a measurable impact on the operations of the community. NIMS is available online at http://www.fema.gov/nims/.

Morning Session – Emergency Response, IC, Local Officials

The incident-response community participation at the morning session primarily represented the perspective of on-scene emergency responders. This would include, for example, fire, police, emergency medical personnel, and other local organizations whose incident response roles find them engaged at the incident site whether as an incident commander, fire fighter, paramedic, or another role. The workshop participants themselves were senior members of these ranks with many years' experience in the emergency-responder roles.

2.1. Fundamental Concepts of Incident Command

The Incident Command System: The Incident Command System (ICS) is the de facto standard for organizing the on-scene incident response command hierarchy. Originally developed as an approach to managing wildfire responses, it was subsequently transitioned to a national standard and has been adopted by many federal agencies. At its core, the ICS defines a basic structure consisting of a Command Staff and a General Staff. The Command Staff includes the Incident Commander (IC), Safety Officer, Information Officer (Public Information Officer under NIMS), and Liaison Officer. The General Staff consists of four sections: Operations, Planning, Logistics, and Finance and Administrative. See http://www.osha.gov/SLTC/etools/ics/ for a detailed description of ICS. Properly applied, ICS can permit the

successful execution of an incident response with significant scope and logistical demands. Effective training in ICS is a strong need within the incident-response community. Notwithstanding its primacy as a standard within the community, ICS is not universally accepted or applied. The New York City 9/11 response is notable (among other reasons) for the fact that ICS was not used uniformly by the responding agencies; FDNY employed ICS while NYPD did not.

Span of control, unity of command: Intrinsic to the formation of an incident-command hierarchy, whether ICS or another structure, are the complementary notions of "span of control" and "unity of command." Span of control defines the maximum number of personnel that may report to a single individual. Maintaining a manageable span of control is critical to successful incident response. Span of control should normally range from three to seven subordinates. The type of incident, nature of the task, safety factors, and distances between personnel and resources all influence span-of-control considerations. "Unity of command" states that each person will report to only one other individual in the command hierarchy. This clarifies relationships and helps to eliminate confusion caused by multiple, conflicting directives.

Emergency Operations Center: An Emergency Operations Center (EOC) is a center that manages resources on behalf of the on-scene incident response agencies. Traditionally, an EOC has been an actual facility suitably equipped with the communications and monitoring equipment necessary to its purpose. The notion of a virtual EOC has recently arisen in which disparate staff are linked via a network and suitably equipped computers. Normally, an EOC is fully staffed only during an incident or during a pre-planned event. EOC's exist at local, county, state or commonwealth, and federal levels. Should it occur that there are multiple incidents in a given geographic area, an *Area Command* is established to handle resource requests and manage competition for resources among the incidents. The Area Command allocates resources on a priority basis. In this scenario, the IC will make requests directly to the area command, which then looks to the EOC to provide the resource. In a hurricane, an event that often impacts large regions and many local communities, local EOCs control their own resources, but the state has control of its own assets and wields ultimate authority over locally based response.

2.2. Establishment and Evolution of Incident Command

Command responsibility initially falls on the emergency responder (ER) first dispatched to the scene of the incident. Upon arrival, that person announces over the radio that he or she has arrived and has established initial command authority. If the initial response consists of multiple people as in the case of a unit of firefighters, then a policy will be in place to determine which of the unit will assume command authority (e.g., seniority). The ER remains as the IC until a formally identified IC arrives at the scene and relieves the ER. At that time, the ER verbally transfers command authority verbally to the new IC. The IC identifies himself or herself. Normally, there is a light atop the IC's vehicle indicating his or her presence and

location; there may be a flag or other marker present or simply a cluster of vehicles.

The identity of the IC may change over time as the incident and the primary emphasis of the response to it evolve. Authority may transfer from a lead agency as its major participation in the response concludes, or new information may be revealed that forces new priorities in the response. The source of greatest threat or risk generally confers command authority on the agency that deals with that type of risk. Often, the IC comes from either the fire department or the police department, although it may come from another jurisdiction such as Emergency Medical Services (EMS), depending on the circumstances of the incident. Policy determines when and how the command authority is transferred.

While it is generally defined ahead of time which agency will lead the response to an incident of a given type (e.g., fire), an incident may encompass multiple jurisdictions, resulting in multiple parallel command hierarchies until a single command can be established.

If police and fire departments are both involved, disagreement over command authority is not uncommon. These agencies do not normally share a unified command, but they may co-locate their IC's. Sometimes competing agencies will "huddle," from which an agreement might emerge on how to cooperatively manage the incident response. As multiple agencies respond to an incident, a certain amount of mutual assessment occurs as ER's communicate and establish their credentials among the aggregated community of responders.

Disputes over command authority in multi-agency responses are not inevitable. Both the FBI and the US Coast Guard train their employees in ICS and both organizations are perceived to work very effectively within the incident-response community. As a result of the East Bay Hills fire of 1991, the state of California enacted the Standardized Emergency Management System (SEMS) to improve response effectiveness in multi-agency and multi-jurisdiction emergencies. SEMS, of which ICS is a key element, is intended to facilitate coordination and information flow among all responding agencies and has been effective in limiting or eliminating disagreements over command authority in multi-jurisdictional responses.

Command authority may also transfer between agencies as the scope of an incident grows. Such growth may cause authority to migrate from the local level to the state level and then up to the federal level. Federal control may be in place from the outset if the incident arises out of a planned event under federal control or if federal agencies are in possession of key information about an incident.

2.3. Multi-Agency and Unified Command

The response to an incident may become "multi-agency" for any of a number of reasons. A national response plan may be invoked that identifies multiple agencies; on-scene personnel may request the participation of additional agencies; personnel (not necessarily on-scene) may learn of sufficient information via the media or other sources to necessitate additional

agencies. For example, in the 9/11 attack on the Pentagon, the City of Arlington Emergency Operations Center (EOC) initiated a response that immediately included local fire and police and the FBI. FEMA personnel, because of their proximity to the incident, arrived and were incorporated into the incident command structure.

It is typically acknowledged that for effective control in a multi-agency response, each functional area in the command structure (operations, logistics, planning, etc.) should reproduce the multi-agency structure down to the lowest levels of the hierarchy. The parallel structures for each agency permit the chain of decision making to unfold naturally. In actual practice, this structure is often not fully realized, leading to inefficiencies as higher level personnel must take on responsibilities that are normally delegated to someone at a lower level.

A *Unified Command* (UC) in which multiple participating agencies efficiently and harmoniously execute command authority is an ideal and typically a goal in multi-agency command situations. NIMS identifies the intent, high-level structure, and recommended operating approach for a UC. However, UC cannot practically be defined in detail for all situations, and in the end, its success relies upon cooperation and collaboration among the participating agencies, so it cannot be guaranteed. Under UC, participating agencies do not cede authority over their jurisdictions, but they must be willing to execute that authority in harmony with other agencies' activities. Bridging the culture gaps between participating agencies is an ongoing problem in the incident response community.

One possible solution to the problem of establishing an overall IC is for the most senior commander to take command as the first among equals. In some incident responses, a single overall authority cannot be established and two or even three IC's will share command. This approach can impair effectiveness by slowing down execution. In such a scenario, the potential exists for the incident to evolve quicker than the multiple-command team can respond.

2.4. Problems and Sources of Failure in Incident Command

The most prevalent source of problems in incident command is communication failure, which can manifest itself in a number of ways: communication hardware failure, intra- and inter-agency breakdowns, and basic verbal misunderstandings, to name a few. There are other sources of problems in incident command as well. As the size of an event grows, so to does the complexity of the response team, creating additional opportunities for failure. The enormous size of hurricane Andrew and the communication failures associated with it begat an evolution in application of ICS. The participation of multiple agencies, especially in a larger event, increases the likelihood of jurisdictional disputes in which one response community refuses to acknowledge the authority of another. In such a case, command can "run off the rails" as tactical decisions are made by an authority not recognized at lower levels of the response hierarchy. A particular variation on the theme of jurisdictional difficulties is the occurrence of an event

on private property where the usual public agency is not the primary responder (e.g., a chemical plant); such scenarios require that protocols be in place to bring in public response support. Since ICS is not universally employed among incident response agencies, there may be incompatibilities in the command hierarchies of the agencies; even where all participating agencies employ ICS, variations in the level of ICS proficiency may be problematic. Managing the expansion of an event to one requiring a large-scale response offers many opportunities for failure, particularly if the event and the flow of information about it are growing faster than the responders can manage. Another problem for larger events is the presence of non-habitual responders that arrive voluntarily but lack a formal means for "plugging in" to the command hierarchy and lack an understanding of ICS. The modern "threat space" includes jurisdictions beyond fire response that gave rise to ICS; at present, for example, there is no national response curriculum for emergent threats such as biological warfare. A characteristic of public health emergencies in general is that they have much slower response times than more common incidents.

2.5. Situational Awareness

Situational awareness is an ongoing need for the response to any event. Emergency responders have a critical role in continuously developing an accurate picture of the event as it evolves. Situational awareness starts with the initial assessment by the first ER responding to an event. That assessment is guided by standard operating procedures that are invoked given the obvious circumstances of the event. It is announced via radio to benefit additional responders en route to the scene. The full dimensions of the event may not be discernable at first inspection, so each ER is trained to size-up the event continuously. If the event grows or if new dimensions are discovered, the on-scene ER's are responsible for conveying current status so additional agencies can be brought in as required. A "large" event may have that designation for any of a number of reasons: spatial extent, multiple different agencies involved, long duration, high complexity. For some events there may be an advance warning that allows some preparation to occur (e.g., hurricane or other observed weather, airplane hijacking).

2.6. Communications and Information Flow

Communicating information is vital to all phases of an event response, and failure of said is an ongoing problem in the response community. Communication failures increase proportionally as the size of the event response grows; the quantity of failures grows also with the size of the community in which the event occurs. In small incidents, communication is typically face-to-face, although two-way radio is a standard communication mode in incident response. Each response community generally has its own communication frequencies and nodes; interoperability is the exception rather than the rule, so "sneaker net" (face-to-face voice communication) is often employed of necessity where multiple agencies are gathered. Communication patterns echo the incident-command structure. The communication chain for *resources* is, in general, dependent on the type of event, the established event chain of command, and it may evolve

over time. Span of control/unity of command constraints establish the lowest-level ER staff as "sensors" and each level in the chain of command as a filtering node; all information is not passed all the way up, only items pertinent to the next level of command. Protocol for information flow up and down the chain of command can overwhelm community resources. Public news media, e.g., CNN, are important to the incident-response community, increasingly so as the size of the event and its response grow. It is not uncommon for information highly relevant to a response to be gleaned from public media. Written documents are an important resource for incident response and are generally in preparation after the first 12 hours of a response.

2.7. Planning

A plan is a skeleton that identifies roles and authority of positions in the incident response team. Over time, politics, personalities, and the evolving event itself will impact a plan and its execution. Pre-planning for known events permits emergency personnel and logistical resources (e.g., maps) to be put in place on-scene prior to the event. Pre-planning for unknown events should consist of developing responses for general types of events (e.g., earthquakes) and should address logistical resources for the locales in which these events might take place (e.g., large assembly areas where more people would be affected if an event occurs such as airports or sporting arenas). Pre-planning also establishes relationships among response personnel prior to the event. Local jurisdictions are not necessarily pleased with Federal planning and involvement in events. Planning failures occur because events may not evolve in anticipated ways. Also, different response communities have their own plans that are not always developed in coordination with one another.

2.8. Existing Modeling and Simulation Approaches

A variety of modeling and simulation approaches are currently in use in the ER community. One common observation is that with a finite number of training venues and an ER population of approximately two-million people, every responder cannot receive all relevant training in a given year.

Tabletop/Sandbox Exercises

A tabletop exercise is essentially a discussion of a response to an event but can also be used to test strategies and procedures. It's not an actual simulation. The participants are together with a discussion facilitator to brainstorm

Command, Control, and Communication and Information Management Tools:
Grease board
Two-way radios
Cell phones
Television
News radio
Emerging technologies
GPS
Visualization tools

tactics, come to know counterparts, and understand mutual expectations and procedures. It is often a catalyst for further discussion. It is not typically inter-agency but can be. With respect to an actual event and response, time in a tabletop exercise is condensed. One fire department has a "sandbox," known casually as "Taylor Town," composed of HO-scale trains and accessories to facilitate such discussions.

Phoenix FD Multimedia Simulator
Phoenix Fire Department has a tactical multimedia fire-only simulator. In collaboration with the Texas Engineering Extension Service, PFD offers the Capstone Program in which other fire departments can travel to Phoenix to make use of the simulator.

US Fire Administration (USFA) Scenario-based Simulations
The USFA's National Fire Academy offers six-day or two-week programs consisting of classroom instruction followed by simulations. The simulations are computer-generated scenarios run and controlled by people. They support multi-agency/multi-jurisdiction participation and can be tailored to local jurisdictions or scaled up to encompass a multi-state region in the simulation. These courses are resource and time intensive. The current on-campus training capacity is approximately 100 classes of 30 to 40 Emergency Response personnel.

US Fire Academy Simulation Laboratory Model City
Within the Fire Academy Sim Lab exists a generic model city for scenario-based training. It is generic because it supports training for teams from all over the country and tailoring it to each community would be prohibitively expensive.

Wildland Fire Training
These are intensive, map-based training exercises for multiple teams. There are two courses: Command and General Staff will train four teams of eight or nine people with up to 60 staff running the exercise; Advanced Incident Management will train up to ten teams with up to 150 staff supporting the exercise. The support staff is separated from the trainees. The courses employ actual tools where possible, with communication by radio, telephone, fax, and role players (e.g., private property owners who provide realistic distractions to trainees). There is little automation, with tactical decisions made by support staff. Random events are injected into the ongoing scenario by controllers, such as communication failures. Events may be invented or may be "replays" of actual incidents. These are felt to be very realistic and excellent training opportunities, but they are so resource intensive that they cannot be run frequently.

WebEOC
This is a commercial web-based tool that simulates EOC functions, including every EOC workstation. It can be used both as a training simulator and as an operational tool. It can be tailored to actual facilities and integrates other electronic technologies such as GIS. It can support simulation of very large incidents. See http://www.esi911.com/.

2.9. Next Generation Simulation Needs

The following sections summarize the discussion of the participants regarding desires and recommendations for future

uses of simulation in incident-management training and execution. They attempt to capture the discussion but do not necessarily constitute recommendations of this report for the purposes of implementation. Chapter 4 presents recommendations for the implementation and use of simulation for incident management training.

Realism

The simulation should model the "rules of the world," i.e., physical processes as well as human cultural and social processes that are removed from immediate scope of the simulation; the simulation should not make decisions or recommendations for the trainees. It must invoke the emotional response of actual events for the trainees. The consequences of trainees decisions must be computed and presented appropriately to trainees in a manner that duplicates as well as possible the feedback channels exercised in actual practice. Similarly, trainees should receive no more information than they would in the field. The simulation should generate spurious occurrences and failures as happens during normal incident response activities. The simulation must permit but not require high fidelity representation of a modeled community, state, or region. It must also accurately represent the level of technology available to trainees in their actual practice, whether that be state of the art or decades old. The simulation must not impose a "correct" solution or preclude the possibility of multiple successful paths as exists in a real scenario.

Flexibility

The simulation must model incidents of all sizes up to and including large scale regional or even national disasters as well as support modeling of the multiple agency jurisdictions involved in a large scale disaster; this implies a scalability to handle hundreds or even thousands of trainees. The simulation must support response community standards but must also be able to model potential technologies that are not yet realized in actual practice. Models must be available for all kinds of incidents including, for example, public health emergencies. It is desirable that the simulation permit utilization as a decision-support tool during an actual event, which implies an ability to incorporate actual data in real-time. Careful consideration must be given to managing simulation time and the tradeoff between temporal realism and the need to accelerate or skip time in order to experience the latter stages of an incident response that could in reality take weeks to arrive at.

Additional Features

In order to help agencies learn how to work together effectively, the simulation should provide a capability to reward effective coordination and communication between responding agencies and, conversely, punish failures resulting from contentious inter-agency relationships. The simulation should integrate instructional capabilities to support learning core competencies for ER's as well as learning NIMS. The simulation should automate control and execution to eliminate dependencies on "back room" staffs during an exercise. Modeling should be accurate and highly flexible to defeat the possibility of "teaching for the test." The simulation must provide record-keeping for simulated resources. It must also be able to record the entire state of an exercise as it unfolds to support after action

reviews and restarts. The simulation should support trainee performance evaluation to enable certification and/or credentialing (in particular, performance evaluations of the IC to date have not been fully successful). It should also support recording of metrics to demonstrate the effectiveness of simulation-based training, evaluate policies, and reveal gaps in current practice.

2.10. Topics for Further Consideration

- Public health, hazardous substance, and biological emergencies
- Tradeoff of the value of high fidelity modeling of responders' communities vs. increased vulnerability from creating detailed infrastructure descriptions that could pass into the wrong hands. A potential solution is to create broad set of generic communities of different sizes over which participating response agencies would lay down their "native" concepts of operation. Note that generic simulations may preclude use as response decision support tool
- Identify opportunities for technologists to observe actual ER training events.
- Modeling issues: local standard operating procedures; scalability and breakdowns of incident command structure as event grows
- Relative roles of EOC(s) and the Area Command
- How well do existing tools support assessment and review, threat and vulnerability assessment, planning, operational decision-making, and resource allocation
- Consider the use of TOPOFF after-action reports as framework for model developers
- Certification of trainees – this is desirable to increase participation but is politically sensitive as it must be bought into by the accrediting agency

2.11. Afternoon Session – State Level IC

The incident-response community participation at the afternoon session represented the perspective of incident-response executives. This includes people with responsibilities at the state level or those with a purview encompassing a regional or major metropolitan focus. Often such personnel are involved in incident response through an EOC.

2.12. Aspects of Incident Response

Information Gathering

An early and ongoing priority is to gather the "Essential Elements of Information" (EEI). EEI identifies "what's happening" with the event and response and are used to support decision makers, inform the press, and frame the event response. EEI comes from multiple sources, including television, web-based and radio media, county-level agencies, local officials, ER's, sensors, citizens (including amateur photography and movies), dispatchers, and various maps of the incident locality (including USGS shake maps). It is important to note that key personnel may be lost or otherwise unavailable during an event. Computer-based simulations, such as the FEMA loss estimation program (HAZUS), may provide useful information. Citizens may provide information, which must be considered with care as it can be misleading or completely false. Sometimes, however, they are the only source of information available. In such

scenarios, their information can neither be overlooked nor treated as reliable and objective. Small communities often enjoy a comprehensive and detailed knowledge of their environs that large cities lack, although all cities have some knowledge of infrastructure and geography available. Another source of information is traffic management cameras that may be employed for surveillance or to reveal current status.

Personnel

Obtaining personnel from emergency support functions (ESF's) to staff and run the EOC is a critical first step. These personnel may originate from a variety of sources such as various state agencies and other organizations that have a vested interest or responsibility associated with the event (e.g., power companies, Red Cross). In New York state, the planning section chief is put in place immediately, then other agencies are contacted for additional personnel. A major event can quickly overwhelm the on-duty staffs of response agencies (police, fire, etc.). There may be policies in place to allow for calling in off-duty personnel. This typically entails documenting the estimated duration of participation and contacting the off-duty staff by pager, phone, or software callback. There may be union issues to consider. Personnel are specialized to particular functions including operations, logistics, planning, and communications. Federal law enforcement personnel should be included in weapons of mass destruction (WMD) scenarios. It is important when assembling a staff that selected personnel be capable of making decisions with only limited supporting information.

Planning, Goals, and Resource Management

Plans may be revealed as too prescriptive, inflexible and unable to scale well, while strategic and tactical goals change as a function of event size. Standard operating guides may be more useful than plans. Emergency response is process independent, not process blind, and there are typically multiple acceptable paths to reach the end of the response. Business continuity plans are developed to identify and safeguard critical infrastructure. Mutual aid agreements are developed (pre-event) between localities to support one another during an incident response by sharing resources. When mutual aid is activated, the provided resource is under command of the requesting agency; dispatchers don't differentiate between resources on the basis of their actual ownership, so they are integrated seamlessly into existing resources.

Community Relations

It is important that incident managers keep the local community informed about the incident and the response to it, as an informed populace is typically more supportive. A potential source of friction for the viewing public arises from their perception of the credibility of television-based experts versus that of response officials. City officials often retain expert knowledge of their local communities. City mayors may be empowered to make evacuation decisions, for which they must be well informed.

Emergency Operation Centers

An EOC will be stood up in response to a variety of conditions including requests from local governments, specific events, pre-defined scenarios

identified by the state, and, in some locations, the elevation of the Homeland Security threat level to a particular level (in New York, yellow or orange levels suffice). EOC's will stand up in advance of known large events (e.g., the Super Bowl) to pre-define logistics and public communications. In New York post 9/11, the EOC will stand up following any significant incident. Former practice was to wait until a request arrived from a local official. In Texas, the State Operations Center (SOC) automatically monitors events having populations of 30,000 or more. In some locations, EOC's are continuously monitored and staffed. Redundant/back-up EOC's are being developed by some states. The EOC's associated with the various levels of government form a hierarchy starting with municipal EOC's at the bottom and continuing up through county, region, and state, although there is some variation from state to state. Resources flow down the hierarchy with state EOC's providing resources for local communities that in turn provide for citizens. Personnel can follow a similar path in that State EOC's may send personnel to help staff local EOC's. Virginia is a commonwealth, which poses particular problems in that the state lacks authority, which is held at the local level. Virtual EOC's, in which multiple disparate centers are united electronically, are growing in popularity (product – WebEOC).

Problems and Sources of Failure During Incident Response

Poor communication is the number one source of failures during a response. Other causes of failure include a lack of understanding of necessary concepts, insufficient training and/or joint training between agencies, a lack of awareness of responsibilities, and inadequate plans (insufficient flexibility or scalability, inadequate technology, duration, or scope). Territorialism and the struggle for authority that it engenders can lead to command and control breakdowns. Similarly, politicians and/or EOC officials may inappropriately attempt to run the incident response. Another difficulty facing incident managers is that their regular responsibilities are ongoing throughout the response, contributing to increased complexity.

2.13. Simulation

Existing Modeling and Simulation Approaches

Current approaches include:

- Table top exercises – these are performed three or four times per year, require about four hours, and may be conducted around an HO-scale city model.
- Functional exercises - conducted in an EOC to put the trainee under realistic stress.
- Full-scale exercises.
- DoD simulations (but there is little opportunity to participate in these).
- Vehicle simulators.
- Computer-based simulations.

Problems with Current Simulation-Based Training

- Too much training is required – participants are "exercised out."
- Limited automation is available.
- Lack of fidelity and realism.
- Poor representation of the response operating environment.

Next Generation Simulation Needs

Realism: New simulation technology should provide a realistic operating environment including the media, noise, equipment and communication failures,

and other distractions or impediments present during an actual response. It should also model the loss of key personnel and knowledge during that occurs in real response activities. Information must be transmitted to trainees using the same modes/channels utilized in a real response. Trainees must be put under stress and need to experience the results of their decisions and actions. The simulation should provide accurate geo-spatial representation of the incident. Play should be unscripted to enable cause and effect of the participants' decisions to drive the scenario forward. Metrics should be available to measure performance in realistic terms (i.e., loss of life and property).

Flexibility: The simulation should be capable of running scenarios based on generic community representations in order to train junior staff in core concepts without the distraction of "native" locations but also be able to run high-fidelity representations for experienced staff to permit training in their regular operating locations. The simulation infrastructure should allow representation of existing technology as well as exercising new concepts, tools, and procedures. The simulation should be both federable and highly scalable to enable simulations of local communities on up through multi-state regions.

Features: New simulation technology should provide incentives to participate such as certifications. The architecture should integrate code to model transport and fate of contaminants and loss estimation models. Accurate resource management for the simulated scenario is necessary, as well as the ability to customize state and local requirements. It may prove useful to couple the simulation to WebEOC. To encourage use and acceptance, the overhead required to set up and run the simulation must be minimized. The simulation should provide a restart/replay capability for decision and consequence review and also to permit experimentation with alternate decisions. The simulation should incorporate some way of rewarding correct performance with respect to some policy. This policy might represent ICS, NIMS, or another approach to structuring a response effort. Voice recognition would be desirable.

Chapter 3. The Role of Computer Simulation in Incident Management

This chapter provides a description of computer simulation technologies and their potential use in all phases of incident management, including training, planning, and incident-management decision support. Much of the discussion below was only touched on during the Workshop itself. The authors of this report prepared this section in order to provide a reference for both incident management professionals and the computer simulation software developers who might engage in the development of simulation tools to support incident management.

3.1 Phases of an Event and Related Activities

The responsibilities of the DHS programs require a wide range of simulation and modeling technologies that vary across the entire spectrum from fast-response, real-time operational simulations to complex high-fidelity simulation activities in support of applied research and development into appropriate technologies. In the context of incident management, there is a critical need for computer simulation capabilities to be used as training, planning, and ultimately management-decision support and response tools. A brief discussion of simulation technologies is included below in Appendix A. A more thorough discussion of simulation technologies applied to DHS needs appears in the report of the October 2003 DHS ASC Computing Program Requirements Workshop.[4]

The four general phases within an event and the activities and/or simulation capabilities that are required are introduced in Table 1. These events include natural disasters, accidents, and terrorist attacks. These phases require the application of incident command, emergency responders, and operational assets to which various forms of simulation and modeling can be applied to support the DHS mission.

3.2 Use of Modeling and Simulation for Training

Training is a traditional and vital component of preparation within the incident-response community. As noted in the previous chapter, simulations are integral to training curricula, but the simulation technologies currently being employed are likely not taking advantage, in most cases, of the full range of capabilities available through computer-based modeling and simulation. Furthermore, we are faced now with conceivable terrorist threats that are unlike any in past experience. Modeling and simulation offers a viable approach to experiencing in some way the range of effects in space and

[4]U.S. Department of Homeland Security Advanced Scientific Computing Program Requirements Worskhop Report, Lawrence Livermore National Laboratory Report UCRL-AR-202297, February 2004.

Event Phases	Corresponding activities/required capabilities
Pre-event	• Vulnerability and risk analysis for sites/infrastructure (urban areas, complex, facility, building, distribution systems, large-scale gatherings/activities, etc.) • Sensor/surveillance design/evaluation R&D capabilities • Sensor/surveillance network architecture and deployment studies • Planning for response to disasters/accident/attack events • Training for all levels of the incident response community • Pre-positioning and activation of EOC and response personnel /assets if appropriate
Event	• Process sensor/surveillance/emergency alerts • Begin first response (fire, police, medical, national assets) and activate ICS, deploy EOC, Area Command if required • Characterize event (natural disaster, accidental, attack) • Characterize accident/attack (chemical, biological, explosives, radiological, etc.), estimate source location of accident/attack if unknown • Acquire real-time predictions of consequences of CBRN accident/attack from operational assets • Select and execute planned mitigation strategies (fire, police, medical, national security assets, system control [e.g. electrical power distribution, facility HVAC, water distribution networks], evacuation/sequestration response, etc.)
Post-event	• Position, stage secondary response personnel/assets • Refine characterization of accident/attack if unknown (source identification, source location, source reconstruction, etc.) • Execute containment strategies if applicable • Initiate investigation of secondary transmission of event consequences (coupled systems failures, spread of infection by various vectors, etc.) • Begin forensics and attribution efforts
Remediation	• Plan remediation effort (structural stabilization/reconstruction, restart systems, decontamination, etc.) • Execute remediation - monitor, evaluate and guide effort • Perform evaluation and initiate new Pre-event planning effort, begin lessons learned activities

Table 1. Event Phases and Corresponding Activities/Required Capabilities

time and the complexity of the catastrophic scenarios presumably being contemplated by our adversaries.

There already exists a large body of simulation software for training, planning, analysis, and entertainment that comprises many features and capabilities applicable to training incident responders. For years, the Department of Defense has aggressively pursued simulation technology to train warfighters effectively and economically, and the entertainment

marketplace has spawned the development of both hardware and software technology to achieve realistic simulations cheaply. ThoughtLink, Inc., under contract to the DHS Office for Domestic Preparedness (ODP), has conducted a systematic "Review of Models, Simulations, and Games for Domestic Preparedness Training and Exercising." For the review, ThoughtLink analyzed 96 products developed by DOD, other government or government-sponsored agencies, and commercial organizations from an initial pool of over 180 candidate products. Aside from the obvious value in surveying and classifying relevant products, ThoughtLink's reports contain a rich body of contextual information that anyone contemplating the development of simulation technology for incident response would do well to review. Among other things, the review lists and discusses a number of benefits that modeling, simulation, and games (MS&G) have to offer the training enterprise:

- Exercise planning – There are a variety of ways the exercise planning process can be enhanced, such as assisting in the development of performance criteria and preparing the evaluator(s) to anticipate responder actions by providing detailed information about the evolving scenario.
- Realism – MS&G can approximate actual conditions and stimulate realistic responses in trainees in a number of ways.
- Safety – MS&G can permit personnel to experience dangerous events without subjecting them to the actual risks associated with the events.
- Frequency – MS&G permits repetition cheaply and reduces the limitations associated with real-world constraints to increase the frequency of training.
- Training and evaluation conduct – Simulation applications can assist training conduct and enhance its effectiveness in several ways, such as providing a trainee monitoring capability, providing real-time reference information resources, and providing real-time performance analysis.
- Automation of data collection – Automated performance data collection can improve data management as well as objectivity in evaluating performance.
- Training for prolonged disasters – MS&G offers a practical way to experience the long-term effects of disasters without investing the actual time duration being simulated.
- Breadth of scenarios and event types – MS&G permits response personnel to experience low frequency/high value type threats.

The latest volume of the review (which has been completed in three phases), as well as the product surveys can be found online at http://www.ojp.usdoj.gov/odp/exercises.htm

3.3 Incident-Management Impact of Using Multiple Levels of Simulation

There are multiple levels at which to apply simulations to support DHS incident management needs. Considering the activities described in Table 1, it is apparent that an overall view of incident management from a simulation perspective requires a system of systems approach. This is illustrated in the following example:

Consider an EOC and incident command that are activated to handle a pre-planned large-scale public gathering (e.g., Super Bowl). The **pre-event** planning phase includes a vulnerability and risk analysis for the site and activity, a design and implementation of sensor networks for identification of threats at critical areas, and a pre-positioning of a rapid response network of security, medical personnel, and response assets. The sensor network design study can be carried out with pre-computed high-fidelity simulations that serve the dual purpose of validating and producing reduced order operational models for use in an actual incident if needed.

If an event occurs, a sequence of sensors alarm, then the pre-planned response activities can be initiated in the event phase. If this is a chemical agent alarm that includes identification and characterization of the agent, a pre-planned evacuation procedure selected by the incident command and enabled by decision support using real-time operational models of source inversion and dispersion predictions can be initiated. Mitigation strategies based on HVAC control for interior spaces can be initiated as well. Pre-positioned personnel and assets can be directed for emergency response and to carry out evacuation and sequestration plans. In the **post-event** phase, simulation assisted source reconstruction and characterization that is consistent with the sensor alarm time history can be initiated to aid in the forensics effort and the containment strategy if appropriate. If appropriate in the remediation stage, higher fidelity forward simulations based on source reconstruction can be used to map contaminant dispersion and to assist in sampling and clean up procedures.

As this hypothetical example points out, there are many places in which simulation can be applied to events within the context of incident management. Clearly the highest-level tools more properly apply to dynamic, virtual scenario, decision-based simulations of systems of systems. These system models of varying fidelity can be used in specific instances to provide appropriate forcing, response and consequence prediction based on decisions made in the incident-management effort. These models must have robust, flexible, interoperable, modular designs that allow coupling or "federation" to other dissimilar modules. In the dynamic training simulation environment, the modules will need to be very robust. In particular, they will need to have extensive capability to function with missing data, failed connections or improper responses from other modules and must proceed with appropriate default actions. In these types of simulations, roles in the virtual event can be populated by personnel that are being trained (students), instructors, adversaries, and possibly virtual or scripted players depending on the goals of the training exercise.

3.4 The Role of Differing Levels of Physical Realism and Simulation Fidelity

Depending on the level of incident-management personnel that is using simulation as a tool for training, planning, or possibly decision support, differing levels of physical realism and simulation fidelity are appropriate.

1) Simulations used at the EOC Level.

Personnel at the Emergency Operation Center and Area Command levels need

to exercise the broadest scope of influence and decision making in managing an event. The highest level of management needs to exercise the entire system of systems view of an event. The virtual scenarios can be a war game type simulation with fellow management personnel, adversarial players (e.g., terrorists) and distracting players as well. The virtual event scenarios should encompass a rich spectrum of events that can have multiple facets that compete for attention, response, and resources. Multi-jurisdictional events would be helpful. The models that are used at the lowest level to force the events (natural disasters [wildfire, hurricane, earthquake, flood, etc.]), terrorist attacks (chemical, biological, explosives, rad/nuc, etc.) and accidents (chemical spills/releases, explosions, etc.) should retain physical realism but provide very fast response. Thus, simulations used at this level will probably need to be simple models of physical reality rather than detailed physics-based simulations. These might be reduced-order models as described above, or other models that are validated either by comparison with higher-fidelity models or physical experiments. These faster models enable multiple events to be exercised to provide training and planning using what-if type scenarios. Note that for training and planning purposes, it may be possible to run more detailed simulations in advance in order to provide information about events in a planned exercise. For real-time incident management, this luxury is not available, and the availability of effective and accurate reduced-order type models will be critical to the success of such tools. The development of such models for real-time incident management is likely to significantly increase the overall development costs for these tools.

2) Simulations used at the Incident Command Level.

Incident commanders need to have IMS capability for a similar range of events as the EOC personnel, but the decision-making scope of these personnel is on a more limited scale. These personnel need to train and plan on responding to more contained or limited events in general with an increase level or physical realism to provide challenges in a spectrum of events that require critical decisions. More physical realism is required to provide training of intuition and experience on events, and their component physical processes, comparable to what responders might encounter locally. These personnel should have access to operational personnel and assets that allow fast, sufficiently accurate, and effective decisions to be made if necessary, e.g., with regards to chemical, biological, radiological or nuclear (CBRN) threats. Simulation used at this level will probably also be based on simpler models of physical reality as in the EOC level, but more attention will need to be paid to the correct simulation of details in an event. As with the EOC level, training and planning tools can make use of pre-computed high-fidelity simulations, while real-time incident management tools will require the (expensive) development of reliable reduced-order type models.

3) Simulations used at the Operational-Response Level.

Operational-response management personnel will require a hierarchy of models of various resolution and realism. These include real-time models

that are consistent with operational decision making during events. The "physics" of these models should be realistic and have a quantifiable accuracy. This is essential for training operational decision makers.

The development of virtual reality training environments is probably appropriate at this level. These personnel should be faced with complex events that challenge the experience and intuition of the operational-response manager; the event, however, should conform to the physical laws of nature. In addition, at this level there is also a value for higher fidelity models that can be useful in planning for pre-scheduled events to design sensor networks and surveillance activities. Having the ability to go through a planning and design process to arrive at a site/facility plan and then to subject this "plan" to various what-if and adversarial-based threats would be extremely valuable.

Chapter 4. Workshop Summary Recommendations for Simulation Usage and Needs for Incident Management Training

Experts at the workshop agreed that incident professionals would increase their proficiency in managing catastrophic events if they train against catastrophic situations that stress their capabilities. Effects and immersion-based simulation technologies create "real-world" environments capable of challenging decision-making skills and accurately presenting the downstream consequences of those decisions. Many professionals will never encounter a truly catastrophic event, yet all professionals must be prepared to meet the demands of these events. Simulations can also reinforce the concepts presented in the National Response Plan (Incident Management and Incident Command Systems).

Incident managers identified several benefits to be derived from computer-simulation based training. These capabilities expand beyond the tabletop exercise capabilities used today:

- Facilitate and promote cooperation in a unified command situation
- Expose emergency responders and incident managers to catastrophic events with large spatial and temporal extents and multiple infrastructure impacts
- Establish and promote interagency communications
- Provide training event cost savings
- Improve training effectiveness and efficiency to minimize "training overload"
- Make effective training more accessible
- Simplify training logistics
- Create a "train-analyze-improve" cycle allowing agencies to realize quantitative and qualitative improvements in their response plans
- Model, analyze, and evaluate new or hypothesized response and incident-management technologies
- Tailor training to the experience level and needs of participants, e.g., basic-response concepts in a generic environment with unclassified infrastructure descriptions vs. specific scenarios with faithful representations of existing infrastructure for event planning
- Provide a capability for better event training After-Action-Review (AAR)
- Present a realistic picture of the situation to each response unit during the training
- Aid in standardization of NIMS and ICS

Workshop participants have a very limited number of simulation tools at their disposal, but they understand the benefits of them. The tools and the training approaches vary from agency to agency and region to region. With a common set of simulation tools, responders could greatly increase the training frequency on interagency exercises for large catastrophic events. Six core areas identified by workshop participants need to be addressed by a suite of simulation tools:

1. Simulation tools must flexibly allow for existing methods of work and support the way in which organizations operate and communicate. Simulation tools need to address how responders

communicate and operate both within and between command structures at the responder, executive, and federal levels. An example is how an EOC, at the local level, would evacuate a city. The EOC might be required to coordinate resources from both the incident commander at ground zero and the EOC at the state office. Practicing this coordination would be possible with simulation tools. Interagency communication like the FBI or Coast Guard, that normally do not participate within the ICS protocol, could be included in simulation exercises, maximizing each agency's ability to respond effectively.

2. **Simulation tools must provide a mechanism for improving incident-management skills, in particular decision-making skills**. Decision-making skills are a key management requirement exercised primarily in a live emergency. Participants claimed that "real-event" decision support is not the objective; computer-training tools are not necessarily appropriate for operations. While this is the current responder paradigm, we believe that good software tools could facilitate operational decisions. Simulations would create the environment to learn, rehearse, and analyze the effects of critical decisions without risking loss of life or property by realistically portraying consequences of decisions. Simulation tools should not replace the decision-making process but should instead allow responders to understand and benefit from the decisions they make. Automated responses used to facilitate training with smaller numbers of people would allow responders to train individually, but it should not be used to replace live input available from users. It is important that the simulation s*tress the players* to give timely, realistic, decisions, rather than well thought out "classroom type" responses. The simulation should clarify and promote NIMS and ICS. Events should be captured to enable analysis and after-action review–giving the opportunity to look at the benefits of alternative decisions.

3. **The simulation must be capable of recreating actual events as case studies**. This will maximize the community's opportunity to experience and learn from a once-in-a-lifetime event. Responders must prepare for events they are unlikely to encounter where the risk of not preparing would have enormous cost. Simulations are an ideal place to capture this data.

4. **The simulation needs to address the distributed nature of the incident-management system**. Exercises will include multiple counties, multiple states, and multiple federal agencies. Users need to be able to work in familiar surroundings with the set of resources available in their everyday environment. This can only be accomplished if participants train from their own facilities with resources they use everyday. Operational resources like faxes, television, and pagers must all be at the disposal of the user to reproduce a realistic scenario and maximize the benefit of an exercise. The solution must be scaleable to handle the large multi-agency demands that current threats impose on us. Large scenarios with many agencies, responders, and resources must scale without performance degradation. A fully flexible solution will accommodate all aspects of the distributed simulation.

5. **The simulation should leverage successful training paradigms such as ICS**. Evaluation of current simulations used throughout the responder community will give insight into the components of a comprehensive solution. Although a simulation should not be a software tool on how to use ICS, its operation should be completely compatible with ICS protocols and it should reveal the benefits of successfully applying ICS in response scenarios.

6. **The simulation should present information in its natural content and format.** A realistic picture of ground-truth familiar to the user is critical for an effective tool. It must include the "noise," misinformation, and normal overloading of information that a developing catastrophic event would contain. Immersion in a realistic environment will produce responses that are more realistic.

Incentives other than federal mandates will facilitate a smooth and successful transition to using NIMS and ICS tools at all levels. Certifications awarded to those proficient in handling large simulated catastrophic events could give responders confidence in managing those events.

Chapter 5. Research and Development Requirements for Advanced Simulation in Support of Incident Management

Experts at the workshop agreed that the development of a limited functionality prototype simulation that creates a realistic simulation-fed training environment is possible in the near term, based on existing simulation technology. Such a prototype could be used in an emergency-management exercise in order to generate more advanced requirements and to develop an understanding of the required path forward for the development of computer-based incident-management training tools. This prototype can also be used as a basis for consideration of simulation tool development for incident-management planning and decision support. However, there are significant gaps in the simulation technology required to develop fully operational capabilities for incident management training as well as for planning and decision support. This chapter summarizes some of these research issues.

5.1 Scalability of Software Solutions

The many dimensions of the problem domain add to the complexity of the envisioned NIMCity simulation environment. In particular, scalability among several dimensions will be a key enabler to the usefulness of the implemented system. In all of these dimensions, numbers are expected to be large, which will dictate constraints on both the software implementation and the computational hardware that must be deployed. A few of the dimensions to be considered are as follows:

- Number of stakeholders and players and their physical proximity
- Number of entities and interactions modeled in the environment
- Number of physical processes or simulations included in the scenario and the fidelity required for these results,
- Number of data sources, (inputs and outputs)
- Incorporation of real-time sensor data
- Network bandwidth and quality of service to the players

5.2 Integration of Multiple Simulation Paradigms

One of the fundamental research challenges embodied in NIMCity is multi-simulation computing. In multi-simulation computing, traditional continuum physics and discrete event simulations are coupled in space and time to model the fully propagated effects and long-term evolution of the system's state from its initial conditions. Multi-simulation computing places a premium on the integration and synchronization of heterogeneous models. Because these models vary widely in what they represent, so may their data input/output requirements, their system resource requirements, their communication requirements, and the length- and time-scales at which they operate.

Many of the necessary individual modeling domains are well known and/or represent active areas of current research. However, federating the computational models from these domains represents a serious challenge that poses multiple questions for the computational science research community.

As a practical matter, the variety of models integrated within a prospective NIMCity framework is too great for any single organization to develop, nor is it practical to discard existing models and develop them anew informed by (as yet undefined) federation requirements; NIMCity must have provisions for incorporating existing models and accommodating their heterogeneous interface requirements. This necessity will add layers of complexity over the lower-level demands of model federation and raises higher demands for effective software engineering as well as organizational collaboration among model providers and NIMCity framework developers.

5.3 Software Environment for Federated Computing

Software infrastructure will play a critical role in reducing the time to solution for development of the NIMCity environment. First, software programming models and design must efficiently harness the underlying computer hardware to ensure reasonable execution performance. Second, software will play an important role in the adaptability of the system to meet the wide range of user requirements for computer platforms and expertise.

Federating the computational and data system across a distributed computational "grid" poses multiple research questions. The ability to federate submodels into an interoperating supermodel is also fundamental. The NIMCity model will be composed of independently constructed *component models*, or *leaf models,* which are then, coupled using higher-level *coupling models* to specify the interactions between components. Federated models must also be federable, so the final model is a hierarchically organized tree of coupling models and leaf models. At runtime, the federation technology will also have to synchronize the coupling models with the component models at a coarse level, while the components are already internally synchronized at a finer level. Some of the component models may be optimistically synchronized, some conservatively synchronized, and some time-stepped. Some may be continuous, others discrete event, and still others agent-based. All combinations of these choices must be supported with the understanding that every additional increment of heterogeneity will cost performance, one way or another.

5.4 Visualization for Insight

An important research challenge is to develop effective representation and presentation of massive multimodal data to aid human decision making and provide insight in the incident handling environment. Consideration could be given to interactive display of large volume of data, immersive visualization environments, distributed collaboratory environments and rapidly deployable visualization systems. These tools need to provide an information rich environment that provides a user with an optimal amount of information with an appropriate context. It must provide this

at interactive rates on typical desktop platforms. Perhaps more importantly, the tools need to provide a high level of semantic-rich interaction. That is the tool must support rapid, streamlined interactive data exploration, allowing a user to gather the information necessary to make decisions at the appropriate level.

5.5 Modeling Human Behavior

All models contain assumptions about human beings, be it an engineer's cognitive model of an equipment failure mode or a model of how people respond to a stimuli. This has two important ramifications for incident management R&D. The first is the need to identify and document behavioral assumptions in models developed for and used in incidence response and management. It is essential that critical assumptions be validated. Where great uncertainties exist about validity, sensitivity analyses should be conducted to determine the importance of the uncertainty in model outcomes.

The second is that we need more robust models of human behavior in emergencies, including models of decision-making, communication, interaction, warning systems, and protective action behaviors. For example, some dose assessment models assume people are passive receptors of an agent, or are located in the same place in the daytime as they are at night. Models based on these assumptions might not apply when people are fleeing or taking precautions in place.

5.6 Understanding Complex Adaptive Systems

Complex adaptive systems are characterized by the interactions of individual agents and elements that tend to self-organize, leading to evolutionary, emerging, and adaptive properties. The envisioned NIMCity simulation environment is an example of such a complex, adaptive system. These systems are subject to revisions as the impact of decisions provides feedback. For these complex adaptive systems, in general, one cannot create a model that accurately predicts the outcomes of the actual system. However, one can create a model that accurately simulates the processes that the system will use in order to create a given output.

5.7 Resource Constrained Computing

The NIMCity models will need to have modes in which they can be used interactively, either (a) for training purposes in advance of a crisis, or (b) during a crisis for operational planning. Both of these modes of interactivity have profound effects on the design of the system. Use of NIMCity for operational planning during a crisis is an even stronger software engineering constraint. Beside the requirements of "training mode," the system's response time has to be bounded by human factors, e.g., the 0.1 second criterion for "instant" response and the human attention span or tolerance for waiting in a pressured situation. Getting both good response time always trades off against throughput. In addition, it may be necessary to be able to trade model fidelity for performance so that decision makers can get a quick approximate answer rather than a slower, better answer. Each of the federated submodels should be parameterized in a way that allows it to run the "same" model with greater or lesser fidelity. There will be many times when it will not be desirable

to run the full-scale infrastructure models because they are too big and slow. For example, if sensitivity studies must be performed, the models may have to be run too many times for full fidelity. Or it may be that one submodel is only capable of a certain degree of fidelity or precision, and there is no point in configuring the others coupled with it to run at any higher fidelity. There may also be occasions when the model's real time performance is critical (e.g., during an emergency) and the fidelity must then be adjusted to fit the time allotted for decision-making.

Relevance of Public HealthIMCity may need to simulate the progression of a large-scale public-health emergency, e.g., an attack on the population with an infectious disease agent. Models of infectious-disease epidemiology generally assume a fixed social landscape in which the public consists of passive bystanders and rational actors who comply with health authorities. It is not clear how well this assumption applies to epidemics of any serious disease, much less ones following terrorist attacks, or the extent to which its validity depends on effective communication by authorities and cooperating media. Some analogies (e.g., Three Mile Island, AIDS or West Nile virus) suggest that episodes of mass panic or hysteria would be rare and localized, while actions based on perceived self and family protection (e.g., evacuation, queries from the worried-well, antibiotic stockpiling) would be widespread. Acts of spontaneous altruism and mutual aid, as well as criminal opportunism and civil disruption could also occur under certain rare circumstances. Insofar as changes in social behavior under stress affect the success of medical and public-health interventions, models used to design them would be improved by incorporating relevant social dimensions.

1. There is a need to develop an inventory of research on the following topics:

- Epidemiological models relevant for bio-terrorism
- Behavioral data for driving the models based on:
    - actual events
    - analogous events
    - research findings
- Case studies of bio-terrorism incidents

2. Behavioral data needs include:

- What is level of quarantine non-compliance? Who? Over time?
- If schools close who will watch children? Will children stay home or go elsewhere?
- If work places shut down, will people stay home? Or congregate elsewhere?
    - What percent will self quarantine?
    - How many would participate in voluntary prophylaxis? Who? When?
    - How many will evacuate area? Timing?

5.8 Relevance of non-Police/Fire/EMS Communities to the Design of Effective Incident Mangement Simulation

Law enforcement, fire/rescue, and emergency medical services (including dispatchers/911 at the local level) are major players in the simulation. However, the response of a number of other personnel may need to be simulated or played during the

simulation. These include the following types of organizations:

- The Office of the Chief Executive.
- Existing planning agencies (e.g., community development, economic development, city planning commissions/municipal planners).
- Hazard mitigation planner/coordinator.
- Local Emergency Planning Committees (LEPC), for hazardous materials (HAZMAT) information.
- Public works agencies and utility companies.
- Social service agencies and volunteer organizations (e.g., American Red Cross, ,Salvation Army, etc.).
- Area hospitals, medical examiner, coroner, mortician, and other appropriate members of the medical community.
- Educational administrators.
- Public Information Officer (PIO).
- Local media.
- Industrial and military installations in the area.
- State aviation authority and/or others connected with provision of air support.
- Port authorities, U.S. Coast Guard station, railways, transportation department.
- The jurisdiction's Chief Financial Officer, auditor, and heads of any centralized procurement and resource support agencies.
- Jurisdiction's legal counsel.
- Labor and professional organizations.
- Organizations in the animal care and control community, including veterinary services.
- Amateur radio/CB groups, such as Radio Amateur Civil Emergency Service (RACES), Radio Emergency Associated Communications Teams (REACT), etc.
- Emergency managers and agency representatives from neighboring jurisdictions, to coordinate mutual aid needs.
- Scientific organizations such as geologists, meteorologists, chemist and etc.
- State and/or Federal representatives, as appropriate.

Chapter 6. Conclusions

The broad conclusion that can be drawn from this workshop is that realistic computer simulation has clear application to Emergency Incident Management, particularly in the areas of personnel training, event planning, and incident-management decision support. This report focused mainly on the application of simulation capabilities to incident-management training support but also touched on the application of simulation to the other areas.

In the homeland security realm, the potential value of realistic computer simulation for training purposes is clear. Incident-response professionals can increase their proficiency in managing catastrophic events if they train against catastrophic situations that stress their capabilities. Immersion-based simulation technologies can create "real-world" environments capable of challenging decision-making skills and accurately presenting the down-stream consequences of those decisions. Since many professionals will never encounter a truly catastrophic event, simulations can be used to prepare those professionals to meet the demands of these events. In particular, such simulations can help assess and improve response plans for catastrophic events. Unlike current training exercises such as TOPOFF, a computer-based simulation does not have to be scripted. Instead, the computer creates an environment that represents the dynamic behavior of the physical environment as events occur and people respond. Since actions of the players in the simulation change the sequence of events, a given event can be simulated multiple times, and the consequences of different incident-management choices can therefore be evaluated.

While it might seem reasonable that simulation tools developed for Incident Management training purposes could be used during an actual event as predictive tools to aid in the decision making process as an event unfolds, the software development requirements for tools that would be required to operate reliably during a crisis would be significantly more stringent and therefore expensive, than those required to develop training software.
This report also concludes that computer software should not be used for the purpose of automatically evaluating performance, either during training or during an actual incident. Because of the lack of foreknowledge and the complexity of these events, replacing expert human evaluation with automatic evaluation of performance would be technologically very difficult and probably not warranted. Expert human judgment should be applied to the evaluation of the success and quality of response by those being trained.

From a technological perspective, computer simulation tools that will allow professionals to train for highly complex and unexpected homeland security events will themselves be highly complex. All aspects of physical infrastructure must be modeled, in addition to the behavior of the population in response to an unfolding event. Each of these aspects will be

modeled separately, and must be coupled together effectively in order to represent the complete reality. While current technology can be adapted to provide some level of catastrophic incident training facility, there are research and development issues that must be addressed in order to provide high-fidelity simulations that are desirable for fully effective incident management training.

Appendix A. General Simulation Technology in Support of DHS Activities.

This discussion will be necessarily brief. It attempts to characterize general DHS simulation technology needs and to indicate the appropriate simulation technologies that can be developed and applied to meet these needs. A more thorough discussion of simulation technologies applied to DHS needs can be found in the report of the October 2003 DHS ASC Computing Program Requirements Workshop.[5]

As discussed in the Requirements Workshop report, simulation technologies have an import role to play in each of the event phases (Table 1) in support of a significant number of required capabilities. These technologies include:

- Continuum (physical phenomenon-based) simulations.
- Discrete simulations.
- High-level simulation technologies and supporting computational infrastructure, such as sensor-driven and hybrid simulations; optimization, inversion, and control methods; verification and validation; and uncertainty quantification.

The continuum physics, discrete simulation and high-level simulation technologies (briefly introduced below) can be viewed as critical computational enabling technologies that address specific required capabilities in the various stages of an event. The overall evaluation and simulation tools that are required to span all or a subset of the activities/capabilities and phases described in Table 1 constitute the domain of incident management simulation (IMS). This IMS technology could be applied for planning, training and eventually as decision support toolsUse of Physical-Phenomenon-Based Simulation Technology

Continuum (physical phenomenon-based) simulation technologies using Partial Differential Equation- (PDE-) and Ordinary Differential Equation- (ODE-) based simulations generally require more computing time and resources than are available in DHS operational environments. These simulations typically require high-performance computing capability well beyond the desktop, laptop or PDA-based platforms that are likely to be used in DHS field applications. Nevertheless, DHS has a strong need for "science-based" simulations incorporating accurate physical models, even if such calculations must be performed off-line (i.e., not in real time). These simulations can support the development of technological solutions to be deployed on the front-lines of our homeland defense. For example, 3-D neutron transport calculations can be performed on a large parallel computer to predict and optimize detector response to a source contained in a geometrically complicated, multi-material environment, thus enabling the design of

[5] U.S. Department of Homeland Security Advanced Scientific Computing Program Requirements Worskhop Report, Lawrence Livermore National Laboratory Report UCRL-AR-202297, February 2004.

better radiation detectors for deployment at the nation's borders. "Full-physics" models also have a role to play in the validation of simpler models that are used in field-deployed technology for DHS and for verification the correctness of software implementations in such technological solutions. However, the use of PDE and ODE simulation technologies to address an emerging threat in real time is more problematic. One currently feasible approach is the development of reduced models that incorporate a phenomenology derived from many high-fidelity (but more expensive) calculations. The reduced models can take a variety of forms including reduced order physics-based and mathematical models, simple rapidly searchable databases and trained neural networks.

In many cases relevant to homeland security, discrete simulations, rather than the continuum simulation technologies (ODE- and PDE-based approaches), will be appropriate. These simulation techniques—also known as discrete-event simulation, agent-based simulation, or entity-based simulation—can be significant in providing technological solutions for DHS. Discrete-event simulation is a simulation of a process or an episode in which distinct events occur. For example, in the context of a biological terrorist attack simulation it might be necessary to model both the deterministic dispersion of an agent (PDE-based) in a public facility as well as the congregation of people at the event, and the subsequent movement of people back into the community (the latter being a sequence of discrete events). For understanding the spread of an infectious disease the secondary transmission of the disease could also be modeled with discrete methods. The most applicable discrete simulation technique is one called an "agent-based model." An agent is a software program defined to represent an important actor in the simulation that interacts with other agents and with their environments. Agents may be people or objects. Agent-to-agent interactions are usually messages created by one agent and sent to another. Agents may also interact with their environments. Environmental variables are usually computed outside of the agent software but may represent an integration of individual agent behavior. Other environmental variables may be the time and day of the week, or current weather conditions. In a simulation, there may as few as a single agent or as many as tens of thousands of agents defined. Modeling large-scale acts of terrorism and their effects are expected to require thousands of agents. Agent-based approaches are expected to provide the most relevant simulation technologies for incident management training applications.

The continuum physics and discrete simulation technologies described above can be coupled and combined with a higher level of simulation technologies to provide capabilities that can make a significant impact in supporting incident management training, planning and response. These methods include advanced scientific computing technologies such as optimization, uncertainty quantification, and sensitivity analysis to help design sensors and sensor networks. For the sensor placement problem techniques such as optimization/inversion, search methods, information theory, genetic algorithms, and combinatorial and discrete mathematics can be applied. In many DHS applications, it is critical to

identify the full range of possible solutions that are consistent with the available data. For example, source localization methods are being developed using optimization and inversion methods for PDE systems and combinatorial- and graph-based methods for network type models. Real-time source inversion capability may require the use of hierarchical physics-based models or mathematical reduced order modeling methods.

Appendix B: Workshop Attendees

Steve Anderson
Lawrence Livermore National Laboratory

Steven Ashby
Deputy Associate Director for Computations
Lawrence Livermore National Laboratory

Budhendra Bhaduri
Oak Ridge National Laboratory

Sandy Bogucki MD, PhD
Yale Emergency Medicine;

Joey Booth

LTC Louisiana State Police

David Brown
Associate Dept Head for Research Computations Directorate
Lawrence Livermore National Laboratory

Brooke Buddemeier
Emergency Preparedness and Response
Science and Technology Directorate
Department of Homeland Security

Brett Burdick
Virginia Department of Emergency Management

Christian Callsen, Jr., LP
Austin/Travis County EMS

James Corones
Krell Institute

Bruce Davis
NASA

Robert Dolci
Chief of Protective Services
NASA Ames Research Center

Amy Donahue
NASA
University of Connecticut

Terry Egan
Emergency Management Division,
Washington Military Department

Lee Erdmann
City of Hartford, CT
Office of the Mayor

Barry Feldman
Town Manager of West Hartford, CT

Martin A. Flemion, III
Deputy City Administrator
City of Laurel, MD

Ludwig Gaines, Esq
City of Alexandria, VA

Randall Griffin
DeWitt NY Fire Department

Paul Hannemann
Texas Forest Service

Gary Hass
Manlius NY Fire Department

Rob Hills
Lawrence Livermore National Laboratory

Tamara Kolda
Sandia National Laboratories, California

Richard Larson
DHS Academic Center of Excellence
Massachusetts Institute of Technology

Paul Lin
Sandia National Laboratories, California

George Maier
FDNY Battalion Chief
Fire Department, City of New York

Celeste Matarazzo
Lawrence Livermore National Laboratory

Michael Mercer
Lawrence Livermore National Laboratory

John Miller
Mississippi Highway Patrol

Craig Moe
Mayor, City of Laurel, MD

Kevin Neary
New York State Emergency Management Office

Jon Olney
FIRESCOPE
Kern Co. Fire Dept, CA

John Perry
DHS/FEMA

Thomas Richardson
Seattle Fire Department

James Schwartz
Arlington County Fire Department

John Shadid
Sandia National Laboratories, New Mexico

Roger Smith
Fire Chief, City of Anaheim, CA

Scott Solomon
International Association of Fire Fighters

John Sorensen
Oak Ridge National Laboratory

Douglas Speck
DHS Science & Technology Directorate

Walt Stoy
University of Pittsburgh - Center for Emergency Medicine

Nancy Suski
DHS Science & Technology Directorate

Bruce Woods
Texas Forest Service and
President of the Texas Fire Chiefs Association

Brian Worley
Oak Ridge National Laboratory

Wayne Yoder
DHS/FEMA/U. S. Fire Administration

Appendix C: Workshop Agenda

AGENDA

Please note - dress is business casual

WEDNESDAY, MAY 12	
Morning session **On-scene Incident Management Personnel** ***Washington Ballroom***	
7:30 - 8:00	Continental Breakfast - ***Ballroom Foyer***
8:00 - 8:30	Welcome/Introduction/explanation of objectives
8:30 - 10:00	Session IA
10:00 - 10:15	Break
10:15 - 11:45	Session IB
11:45 - 12:00	Wrap-up/next steps
12:00 - 1:00	Lunch (*morning session participants only*) - ***Promenade***
Afternoon session **Incident Management Executive Level Personnel** ***Washington Ballroom***	
1:00 - 1:30	Welcome/Introduction/explanation of objectives
1:30 - 3:00	Session IIA
3:00 - 3:15	Break
3:15 - 4:45	Session IIB
4:45 - 5:00	Wrap-up/next steps
5:00 - 6:00	Reception (*afternoon session participants only*) - ***Mayfair Court***
THURSDAY, MAY 13	
Synthesis / Report ***Washington Ballroom***	
7:30 - 8:00	Continental Breakfast - ***Ballroom Foyer***
8:00	Discussion begins