Distributed Simulation - A Necessity Or Ivory Tower Research?

Charles McLean
National Institute of Standards and Technology
Gaithersburg, MD 20899

For what kind of applications distributed simulation will be an absolute must?

There is a growing need for the nation to be better prepared to deal with both man-made and natural disasters. The responses to the attacks on the World Trade Center and Hurricane Katrina are strong evidence of this need. Effective emergency response presents a number of challenges to the federal, state, and local government agencies. First responders and incident management personnel need better planning and training resources to prepare for future incidents. One major challenge is the lack of time and opportunities to train the emergency responders and decision makers to handle emergencies. Another challenge is the variety of different types of disaster scenarios that must be dealt with. Yet another is the complexity of organizations and systems affected by and involved in responding to disasters, see the National Incident Management System (NIMS 2004) and the National Response Plan (NRP 2006).

Live training exercises while valuable are often very expensive to organize and conduct. The limitations of live exercises could be overcome through the use of integrated modular simulations that model the major phenomena and incident response operations associated with a disaster. Planning and training systems that are based upon simulation technology could help to prepare for a more diverse range of scenarios than live exercises. These systems could also support individual, team, or multi-organizational planning and training needs at lower cost. Distributed simulation will be an absolute must to support preparations for disaster incident management and emergency response operations.

Why this is the case?

Distributed simulation could help address many of the challenges that we face today. Why build distributed rather than monolithic simulations? A distributed approach could enable the integration of modules created by different developers and enhance overall functionality of planning and training systems. For example, distributed simulations could be used to:

- enable parallel, modular development of specialized simulation system components by independent software developers with different areas of expertise.
- allow the configuration of integrated simulations that meet specific regional or scenario-based needs.
- model multiple organizations where some of the information about the inner workings of each organization may be hidden from other participants for reasons such as security or proprietary issues.
- simulate multiple levels of organizations and systems at different degrees of resolution such that lower level simulations generate information that feeds into higher levels.
- model multiple systems with different simulation requirements where an individual simulation-vendor’s products does not provide the capabilities to model all areas of interest.
- allow software developers to hide the internal workings of a simulation system through the creation of run-time simulators with limited functionality.
- create an array of low-cost, run-time, simulation models that can be integrated into larger models.
- take advantage of additional computing power, specific operating systems, or peripheral devices (e.g., virtual reality interfaces) afforded by distributing across multiple computer processors.
- provide simultaneous access to executing simulation models for users in different locations (collaborative work environments).
- offer different types and numbers of software licenses for different functions supporting simulation activities (model building, visualization, execution, analysis).

The behavioral,phenomena, and response organization simulations may be large, complex, and expensive to model. For example, some of the different types of simulators that may be included in emergency response planning and training simulations are:

- *Social behavior* – models the collective social behavior of multiple individuals including crowds, traffic, epidemics, and consumer behavior.

- *Physical* – models the physical phenomena involved in the creation and growth of the emergency incident including earthquakes, explosions, fires, chemical, biological, or radiological plumes.
- *Environmental* - models the environmental phenomena that may affect the growth or containment of the emergency incident, its impact on the population or on the efforts by responding agencies including weather, watershed systems, indoor climate, and ecology.
- *Organizational* – models the actions of the organizations involved in any aspect associated with the incident including fire departments, law enforcement, health care, other government agencies, and even terrorist organizations.
- *Infrastructure systems* - models the behavior of the infrastructure systems following the occurrence of an emergency incident including the propagation of the impact of damage throughout systems such as power distribution, water and food supply, computer and communications networks.

A survey (Jain and McLean 2003) indicates that a number of modeling and simulation applications for analyzing various disaster events already exist.

What has to be done to make it happen?

A coordinated effort by developers, government agencies, and standards organizations will be required to achieve the vision of interoperable simulation-based planning and training systems. More effort will need to be put into the following areas:

- Development of technically correct models, behaviors, and data for various phenomena that affect training, mission planning, and operational support.
- Use of gaming technology to provide an immersive, engaging graphical, audio, and haptic (force feedback) environment that offers high quality realistic experiences.
- Enhancement of distributed simulation mechanisms that enable time synchronization, data sharing, check-pointing, time warp, rollback, replay, and logging functions between various simulation and gaming applications.
- Implementation of mechanisms that allow for centralized distribution and management of updates to software and data sets.
- Establishment of security features that prevent unauthorized access to, or modification of, computer systems, software, and data.

Effective, technically sound, and commercially-available data standards will also be needed. Examples of data types that will need to be standardized:

- *Incident management structure:* organizations, roles, responsibilities, policies, plans, procedures, actions, records, resource allocations, checklists
- *Response resources*: organizations, equipment, systems, vehicles, people, evacuation centers, supplies, contact points, data, capabilities, resource capacity, status
- *Infrastructure systems*: transportation (roads, trains, buses, trucks), telecommunications, power, gas, water, food, healthcare, sewage, alerting systems, status, sensitive targets
- *Spatial data*: maps, terrain, regions, areas, and building layouts and models
- *Hazard effects:* chemical, biological, nuclear, fire, severe weather, other natural and man-made disasters, plume models, flooding, health
- *Incident events:* chronologies, timing, descriptions, victims, damage assessments, and other status data
- *Responder computing and communications:* radio and other equipment, channel assignments, switching systems, transmission towers, areas of coverage, message formats
- *Population and demographics:* location, age, sex, other attributes by time of day
- *Weather and environmental* – wind speed, air temperature, precipitation.
- *Financial:* cost of operations, consumables, leased equipment, labor.

Although a number of standards development efforts are underway, much more needs to be done. Standards will need to be harmonized. Validation, verification, and testing capabilities will need to be established as well to ensure correctness and interoperability of simulations.

References

Jain, S. and C.R. McLean. 2003. Modeling and Simulation of Emergency Response: Workshop Report, Relevant Standards and Tools. National Institute of Standards and Technology Internal Report, NISTIR-7071. Available via <http://www.nist.gov/msidlibrary/doc/nistir7071.pdf>

National Incident Management System (NIMS 2004). http://www.fema.gov/emergency/nims/index.shtm

National Response Plan (NRP 2006). http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm.

CHARLES R. MCLEAN is a computer scientist and Group Leader of the Manufacturing Simulation and Modeling Group at the National Institute of Standards and Technology. He has managed research programs in manufacturing simulation, engineering tool integration, product data standards, and manufacturing automation at NIST since 1982. He has authored more than 50 technical papers on topics in these areas. He is on the Executive Board of the Winter Simulation Conference and the Editorial Board of the International Journal of Production, Planning, and Control. He is formerly the Vice Chairman of the International Federation of Information Processing (IFIP) Working Group on Production Management Systems (WG 5.7). He holds an M.S. in Information Engineering from University of Illinois at Chicago and a B.A. from Cornell University. His e-mail address is <mclean@cme.nist.gov> and his web address is <http://www.mel.nist.gov/msidstaff/mclean.chuck.html>.