A Taxonomy of Homeland Security Modeling, Simulation, and Analysis Applications

Charles R. McLean
Sanjay Jain
Y. Tina Lee
National Institute of Standards and Technology
Gaithersburg, MD 20899, U.S.A.
301-975-3511, 301-975-5748, 301-975-3550
mclean@nist.gov, sanjayj@nist.gov, leet@nist.gov

Keywords:
Homeland security, taxonomy, classification, simulation, interoperability, and standards.

ABSTRACT: *The effective use of modeling, simulation, and analysis (MSA) applications could greatly enhance our ability to carry out the homeland security mission. These applications can be used to evaluate vulnerabilities in the nation's critical infrastructure as well as engineer security systems to respond to those vulnerabilities. They can also be used to train participants in the National Incident Management System and assess their performance, plan operations such as responses to terrorist attacks and natural disasters, and support decision-making processes within homeland security agencies. Currently, the development of MSA tools has been conducted largely on an ad hoc and piecemeal basis. There is very little, if any, coordination of MSA development activities across government agencies, the research community, the commercial software sector, and various standards organizations. Without coordination and appropriate standards, there is little possibility of software re-use or the establishment of reference data sets that meet homeland security needs. This report describes a taxonomy, or classification system, of MSA application areas that are critical to meeting homeland security needs. The taxonomy will be used to classify applications and develop requirements analyses for those applications. These analyses will in turn be used to identify a recommended suite of existing standards and standards gaps that must be filled. With these standards recommendations, agency program managers, software developers and standards development organizations can work together to resolve interoperability issues between MSA software applications and achieve better re-use of software and data sets.*

1. Introduction

The potential applications of modeling, simulation and analysis (MSA) techniques in the area of homeland security are tremendous. For example, MSA tools can be used to train incident management personnel, to support the engineering and implementation of new security systems, and to help planners make more effective decisions, among other functions. Government contractors, national laboratories, academic researchers, and independent private software developers have already created a large number of models, simulations, and analysis tools to meet these needs. In 2003, NIST held a workshop to bring together experts in the field and documented needs and some 63 existing applications [1]. Since that time, many new MSA applications have been developed and the number of implementations grows every day. Much of this development work is going on independently outside of DHS.

Unfortunately, the entire MSA development process is being conducted on a largely ad hoc basis with little or no coordination between sponsoring government agencies, the research community, software vendors, simulation users, and other interested parties. Furthermore, a very large number of federal, state and local agencies are responsible for aspects of homeland security and emergency response operations. Each organization may have different needs, as well as a different understanding and appreciation for the use of MSA techniques. One of the major challenges for mounting a coordinated effort is that there is no common framework and associated terminology to identify all the potential applications for MSA techniques. As such, there is little possibility for the re-use of existing software modules and data sets, or interoperability between products developed by different organizations. It is even difficult to determine what applications might be currently available to meet a particular training need or support a specific system-engineering project.

A common taxonomy, or classification scheme, is urgently needed to help categorize the existing and potential uses of MSA applications for homeland security. The taxonomy would help organizations identify and communicate their MSA needs and existing applications in a manner that everyone can understand. More importantly, the common understanding can be used to identify and prioritize missing MSA applications and standards that would help improve homeland security capabilities.

The DHS Science and Technology (S&T) Directorate has recognized that there is a critical need to establish order and appropriate standards for the homeland security modeling and simulation domain. NIST has been tasked with coordinating the identification of standards that are needed to improve the efficiency of MSA application development and the utilization of homeland security modeling, simulation, and analysis products. The first step in the NIST plan to improve the effectiveness of homeland security MSA applications is to establish mechanisms that will help track what technology is current available and best practices are currently employed by simulation developers. Longer-term objectives include the identification of standards gaps that need to be filled and recommendation of verification, validation, and accreditation (VVA) procedures for MSA.

The first step is to develop taxonomy for categorizing homeland security models, simulations, and analysis applications by various key characteristics. This document describes the proposed taxonomy, rationale for the classification scheme, and a description of some high level characteristics. The intention is to have a classification scheme that will hopefully stand the test of time and not require frequent modification as needs change and new applications are developed. The document is not focused on evaluating or defending particular uses of modeling and simulation, but rather providing a scheme for classifying applications, recognizing the fact that these applications already exist, are currently in development, or may be developed in the future.

Due to the international interest in the homeland security area and the potential international market for relevant products, it is desirable to have a scheme that can be used by the U.S. and other nations as well. A generic classification scheme has been proposed. The document and proposed taxonomy will be reviewed and amended by a panel of experts from various organizations within the homeland security community as soon as it reaches a smooth draft form. The categorization scheme may be subsequently submitted for standardization by an appropriate standards body such as the Simulation Interoperability Standards Organization (SISO).

1.1 Modeling, Simulation, and Analysis Issues

Simulations may be used as executable models of the real world or experimental laboratories that support various homeland security planning, training, and analysis needs. A recent report by a blue ribbon National Science Foundation panel on Simulation-Based Engineering Science (SBES) reported as its major finding *"SBES … is central to advances in biomedicine, nano-manufacturing, homeland security, microelectronics, energy and environmental sciences, advanced materials, and product development* [2]*."* A 2002 National Research Council report [3] noted the importance of simulation, analysis, and modeling tools to homeland security: **"***Systems analysis and modeling tools are required for threat assessment; identification of infrastructure vulnerabilities and interdependencies; and planning and decision making (particularly for threat detection, identification and response coordination). Modeling and simulation also have great value for training first responders and supporting research on preparing for, and responding to, biological, chemical and other terrorist attacks."* Although there have been many MSA applications that support homeland security needs which have been developed with and without government support, there has been little or no attempt to coordinate or maximize the benefits of those development efforts.

But what precisely do the terms modeling, simulation, and analysis mean? As defined by Banks [4], simulation is: *"…the imitation of the operation of a real-world process or system over time. Simulation involves the generation of an artificial history of the system and the observation of that artificial history to draw inferences concerning the operational characteristics of the real system that is represented. Simulation is an indispensable problem-solving methodology for the solution of many real-world problems. Simulation is used to describe and analyze the behavior of a system, ask what-if questions about the real system, and aid in the design of real systems. Both existing and conceptual systems can be modeled with simulation."*

The Department of Defense (DoD) defines modeling as the "application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process [5]. DoD defines simulation as "a method for implementing a model over time [6]." U.S. Navy defines modeling and simulation as "the use of models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making managerial or technical decisions. The terms "modeling" and "simulation" are often used interchangeably [7]." In the context of modeling and simulation, analysis refers to the study of the data output through execution of simulation models to determine a number of quantitative and qualitative measures of performance and underlying relationships. The analysis should lead to insights in to the behavior of the system being modeled. Experts often identify simulation as a type of analysis tool [8]. Examples of types of analysis tools include one-sided analysis, game-theoretic analysis, optimization, exploratory analysis, rational-analytic decision analysis, and subjective portfolio balancing.

MSA applications are of little value if there is not a high degree of confidence in their results. How do we know that a model or a simulation is correct? VVA is the mechanism that is used to maintain quality control. VVA terms are defined as follows [9]: Verification is the process of determining that a model implementation accurately represents the developer's conceptual description and specifications that the model was designed to. Validation is the process of assessing whether a model or simulation is an accurate representation of the real world given its intended uses and establishing a confidence level for that assessment. Accreditation is the formal certification that a model or simulation is acceptable for use for a specific purpose. Accreditation is conferred by the organization best positioned to make the judgment that the model or simulation in question is acceptable. An accrediting organization may be an operational user, a program office, or a contractor, depending upon the purpose of the model or simulation.

1.2 Software Interoperability, Reuse, and Standards

Many MSA software applications have been developed or are currently under development. Presently, there is little likelihood that these systems will be capable of being integrated or readily adapted to support different local needs of incident management organizations across the nation. MSA tools, like any other software applications, are costly to develop and may be impossible to integrate if they are independently created by different organizations. If costs are to be reduced, it is critical that redundant software development efforts be minimized. Paying two or more times for the creation of similar software applications wastes valuable resources.

Consensus standards are needed to enable and encourage software and data re-use. What needs to be standardized? Standardization of integration architectures, specifications of module scope and functionality, data interfaces and protocols, application programmer interfaces (APIs), VVA procedures and other test methods, test data sets, and other interoperability mechanisms would help maximize the potential of MSA applications. Standards may result from consensus standardization processes within standards development organizations (SDOs), DHS mandates, or interfaces that are defined by commercial developers that are accepted as de facto standards. The taxonomy described in this paper is a first step towards categorizing the great variety of homeland security MSA applications so that systems with similar needs can be grouped and standards gaps identified.

1.3 Classification Schemes

In the 18th century the biologist Carolus Linnaeus stated, *"The first step of science is to know one thing from another. This knowledge consists in their specific distinctions; but in order that it may be fixed and permanent distinct names must be given to different things, and those names must be recorded and remembered."* Linnaeus was responsible for developing a categorization system for living things [10]. Categorization is the process of recognizing, differentiating, and understanding objects for a specific purpose. Categories should shed light on the relationship between the subjects and objects of knowledge. Categorization is fundamental in language, prediction, inference, decision making and in all kinds of interaction with the environment [11]. A number of classification schemes have been developed that are in use every day. Government and industry use the North American Industrial Classification System (NAICS) to classify businesses. Manufacturers use group technology classification and coding systems to classify products, retrieve and reuse manufacturing knowledge, specify manufacturing processes, and design production facilities.

The technical focus of this paper is to provide an overview of a MSA applications classification system or taxonomy for homeland security. The taxonomy will shed light on the characteristics that define these applications. Such a classification system will help the community recognize similarities and differences between these applications. It will provide a basis for defining functional/data requirements for applications and facilitate the development of needed standards.

1.4 Overview of the Paper

This paper represents an abbreviated version of a draft NIST technical report that fully defines the proposed classification scheme for MSA applications. A brief summary of the structure of this document follows. The succeeding sections of this document discuss proposed taxonomy or classification scheme. Wherever possible and appropriate, established DHS terminology is used to define MSA characteristics. An enumeration of all of the taxonomic classification codes cannot be given due to the space limitations of this document.

Section 2 defines objectives for modeling, simulation, and analysis applications, i.e., the reason the application was developed. Section 3 identifies target user organizations for the MSA application and keywords for describing the missions of those organizations. Section 4 describes aspects of the simulation domain or context of the application. Section 5 provides a summary of possible implementation characteristics that may be captured in a database of applications. Section 6 presents conclusions. The last section of the document provides references.

The authors welcome comments or feedback on the proposed taxonomy and discussion of attributes. Review workshops are planned to obtain expert feedback from the homeland security community. Instructions for submitting comments may be found at www.nist.gov/simresponse.

2. Modeling, Simulation and Analysis Objectives

A MSA application is often developed to satisfy a single major objective, for example the training of incident management personnel. This characteristic identifies the primary purpose of an MSA application. Application objectives are likely to be mutually exclusive, e.g., a training system would probably not be used for systems engineering and vice versa. Potential users looking for systems that are available to meet a specific need will typically want to search for an application based on its defined objective or original intended use. The major categories of objectives that have been identified are:

- Decision Support
- Planning Levels and Domains
- Intelligence and Risk Analysis
- Systems Engineering
- Training and Performance Measurement
- Component Module

Each of these MSA objective types is described in more detail below.

2.1 Decision Support

A major objective of MSA applications is decision support. Human decision-makers face a wide range decisions in the context of homeland security, ranging from simple to complex. MSA can assist personnel in making decisions such as where to allocate budgetary funds for maximum impact, which surveillance option will provide better security for a location, or what is the likelihood of a particular type of incident or natural disaster occurring in a region given historical data.

Decisions are simply choices made between alternatives based on a careful estimate of the pros and cons of each alternative. Decision support means helping an individual or a group to gather intelligence, generate alternatives, and make informed choices through estimation, evaluation, and comparison.

Zachary [12] identified six types of cognitive support that is needed by human decision-makers:

- Process models, e.g., simulations
- Choice models, e.g., decision trees with expected value calculations, analytic hierarchy process.
- Information control techniques, e.g., data fusion tools.
- Analysis and reasoning techniques, e.g., cause-effect diagrams, numerical optimization and statistical analysis;
- Representation aids, e.g., data visualization tools.
- Human judgment amplifying/refining techniques, e.g., expert-guided optimization, Bayesian updating.

A number of different classification schemes have been defined for categorizing decision support functions, but there is no commonly accepted agreement one scheme.

2.2 Planning Levels and Domains

MSA applications that support planning may be characterized by a planning level and a domain. The DHS Presidential Directive 8 Annex 1 defines four planning levels *strategic, concept*, *operations*, and *tactical* [13]. Business planning texts typically divide the planning problem at each level into different domains that may require specialized expertise, e.g., finance.

Strategic refers to a plan that defines the mission, identifies authorities, delineates roles and responsibilities, establishes mission essential tasks, determines required and priority capabilities, and develops performance and effectiveness measures. *Concept* refers to a plan that briefly describes the concept of operations for integrating and synchronizing existing Federal capabilities to accomplish the mission essential tasks, and describes how Federal capabilities will be integrated into and support regional, state, local, and tribal plans. *Operations* refer to a plan that identifies detailed resource, personnel, and asset allocations in order to execute the objectives of the strategic plan and turn strategic priorities into operational execution. An operations plan contains a full description of the concept of operations, including specific roles and responsibilities, tasks, integration, and actions required, with supporting support functional annexes as appropriate. *Tactical* refers to the detailed development and identification of individual tasks, actions, and objectives tailored to specific situations and fact patterns at an operational level. Tactical planning is meant to support and achieve the objectives of the operations plan.

Examples of planning domains include products and services; financial and budgeting; organizational (structure, staffing, training, communications, and coordination); facilities and equipment; technology (trends, research and development); marketing (forecasting, media interactions, promotion); and legal, to name a few.

2.3 Intelligence and Risk Analysis

Intelligence and risk analysis is another possible use of MSA applications. As an intelligence tool, MSA may be used to identify anomalous behavior indicative of impending incidents. For example, analysis techniques may be used for determining whether an increase in number of patients with selected symptoms should raise a flag or is an acceptable occurrence. Risk analysis includes assessment of the probability of unfavorable outcomes based on the gathered intelligence or planned actions. For the preceding example, risk analysis can be used to determine the risk of a wider epidemic based on the identified delivery of bio-agent leading to increase in patients with the specific symptoms and the reduction in risk if mitigation actions are implemented. Similarly, factors indicative of natural incidents such as impending spread of bird flu may be tracked and analyzed.

2.4 Systems Engineering

Another major objective that MSA applications support is systems engineering. The proper use of MSA applications can greatly enhance our nation's abilities to develop new systems that are needed to support homeland security. Systems engineering is an approach for organized development of a product or service through its life cycle. It includes approaches for capturing and analyzing requirements and tracking the development of systems against a set of requirements through design, test, evaluation, and operation. The DoD has been a leader in applying MSA technology to systems engineering. DoD's Defense Acquisition University states, "*A system* is *an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective. Systems engineering consists of two significant disciplines: the technical knowledge domain in which the systems engineer operates, and systems engineering management. …Modeling and simulation has become a very important tool across all acquisition-cycle phases and all applications: requirements definition; program management; design and engineering; efficient test planning; result prediction; supplement to actual test and evaluation; manufacturing; and logistics support. With so many opportunities to use M&S, its four major benefits; cost savings, accelerated schedule, improved product quality and cost avoidance can be achieved in any system development when appropriately applied.*"

MSA applications can be used to help define needs and specify detailed requirements, conceptualize and evaluate alternative solutions, enable rapid development of system prototypes, and provide a virtual test environment once actual systems have been implemented.

2.5 Training and Performance Measurement

A common objective of simulations is to provide an environment for training and performance measurement. DoD has long recognized the value of simulations in preparing the military for future conflicts. Simulations provide risk free environments exposing trainees to real life conditions. Simulations enable trainees to rehearse and evaluate strategies, make decisions, and perform actions in a variety of situations, without paying the serious consequences that may befall them in the real world. In addition to providing an environment for classroom instruction, simulation can also be used for performance measurement, i.e., testing the readiness of individuals or teams to perform in real environments that cannot be implemented through other means. For example, testing a management teams ability to respond to a natural disaster such as a hurricane.

Eleven common classes of training objectives were defined by Bloom [14] and are frequently used by experts in the field of education: recalling bodies of knowledge, using verbal information, rule learning and using, decision making, detecting, classifying, identifying symbols, voice communicating, recalling procedures and positioning movement, steering and guiding, continuous movement, and performing gross motor skills. Each of these characteristics is identified in the taxonomy under training and performance measurement. More detailed decompositions of these characteristics have also been defined by educational experts and are included in the taxonomy.

2.6 Component Module

MSA applications that are not intended for stand-alone use in the homeland security domain are categorized as component modules. Component modules may be assembled into larger applications to satisfy one of the other objectives outline above. Models of phenomenon, organizations, and functions that are not directly involved in homeland security may be built as component modules that may be used by one or more other MSA applications. For example, a weather simulation may be utilized in conjunction with a plume simulation model to estimate the exposure of population to a toxic agent. A stand-alone weather simulation in itself would probably not satisfy a major homeland security objective, but might be categorized as a component module if it was designed to be used with other simulations, such as a hurricane response trainer.

3. Target Organizations and Missions

MSA applications are typically developed to meet the needs of specific organizations or groups of users. For example, a system simulation of a baggage scanner would support organizations responsible for airport security. In the U.S., this would be the Transportation Security Administration, but in another country the agency may have a different name or may be a contractor. The specific names given to organizations often change across governmental jurisdictions and geographic boundaries. To ensure that the classification scheme has widespread applicability, generic attributes, rather than specific names, are used to identify target organizations for MSA applications.

The generic characteristics that describe target organizations are the type of organizational entity, the level or scope of the organization, the persistency of the organization over time, and its mission key words. Types of organizations include various governmental and non-governmental entities:

- Multinational bodies (e.g., United Nations, North Atlantic Treaty Organization)
- Governmental agencies or departments
- Military services (e.g., Army, Navy, Marines, Coast Guard, Air Force, National Guard, militia)
- Private sector organizations (e.g., commercial or for-profit corporations, public utilities, non-profit charities and foundations, volunteer groups).

Level or scope is used to identify the hierarchical level or scope of responsibility for the entity, such as: international; national; state, provincial, or tribal; regional; county; city, township, or village; and other lower level associations (precinct, school district or school, community, residential development). Persistency over time for the organization is used to specify how long the organization is expected to exist, for example: permanent; temporary (limited or fixed duration, e.g., contractual period); and ad-hoc or event-based.

Mission key words are used to identify at a high level the types of mission areas that are associated with the organizations for which the application is targeted. Examples of mission key words include: agriculture, communications, community services, construction, crisis management, defense, education and training, emergency response, energy, entertainment, environmental, financial or economic, food distribution and services, justice or legal, land management, law enforcement, manufacturing, medical and healthcare, mining and natural resources, political, public works, religious, research and development, safety, science, engineering, and technology, seas and waterways, security, transportation, utilities.

4. Simulation Contexts

The context identifies the nature of the simulation, i.e., the major aspects of the homeland security domain that are simulated by an application. Aspects of a simulation context include modeling domains; types of incidents, events, and activities; emergency support functions; and life cycle phases. The modeling domain gives an indication what is being simulated or the dynamics of the simulation, i.e., the ways in which real world behaviors, processes, or phenomena are generated. For example, the domain may be modeling the behavior of individuals, organizations, physical devices, or the environment. Examples of incidents or events include natural disasters, terrorist attacks, and industrial accidents. Emergency support functions include emergency management, public safety and security, search and rescue, and fire fighting. Life cycle phases are defined as prevention, preparedness, response, recovery, and mitigation. A particular simulation application may be characterized by multiple attributes in each aspect area. Each of the major aspects of the simulation context is described in more detail below.

4.1 Modeling Domains

A modeling domain defines the type or types of behavior, phenomena, processes, effects, etc. that are simulated within the application. Major groupings of modeling domains for categorizing simulations include *Social Behavior; Physical Phenomena; Environment; Economic; Organization; Infrastructure System;* and *Other System, Equipment, and Tools.* Each grouping and examples of the types of simulations within each grouping are described below. For a more detailed discussion of the different types of simulators, see [15], [16].

Social Behavior models human interactions based on mental perspectives, decisions, and actions of multiple individuals within a certain context, e.g., at a public event, on the roadways, or at grocery stores. The simulation typically involves the interaction of individuals leading to a collective behavior or phenomena. Examples of social behavior simulators include those that model crowds, traffic, epidemics, and consumer behavior.

Physical Phenomena models various non-human phenomena associated with the origin and propagation of emergency incidents. They may determine the extent of the damage to structures and feed damage data to other associated simulators. Examples of physical phenomena simulators include earthquakes; explosions; fires;

chemical, biological or radiological plumes; disease and bio-agents; and biotic agents.

Environment models a particular ecosystem or closed environment that may affect the growth or containment of the emergency incident, its impact on the population, or the efforts of responding agencies. Such environmental phenomena include atmospherics, climate, and weather; watershed systems; land contamination; indoor climate; and ecology.

Economic models the impact of an incident or a policy on the economy of interest. Economic models are usually classified based on the technique used such as substance flow analysis, life cycle assessment, partial economic equilibrium analysis, or using the level of analysis such as macro versus microeconomic models. Sector specific models will be useful for understanding the impact of incidents and policy changes on relevant economic variables such as demand and supply of goods within the sector.

Organization models the functioning of the organizations involved incident management or impacted by an incident. They may model the flow of information within the organization, flow of authority, decisions, and resulting actions. They typically will utilize the relevant policies, procedures, and operating rules to model the actions of an organization and its members. Example simulators include fire departments, law enforcement, health care institutions, government agencies, military units, businesses, voluntary assistance, and terrorist organizations.

Infrastructure System models the behavior of systems such as food supply chain, energy distribution, water supply, transportation, computer and communications. They may model the propagation of the impact of damage through out the infrastructure system based on the damage to one part due to the emergency incident.

Other System, Equipment, and Tool model various devices to support other simulations or systems engineering processes. Some examples of the types of entities that may be modeled include: aircraft; bomb disposal; construction equipment; fire fighting equipment; hazardous material decontamination and disposal; material handling systems; medical systems; personal protective equipment (PPE); search and rescue equipment; security systems; sensors; ships and other watercraft; test equipment; and vehicles.

4.2 Incidents, Events, and Activities

Another major element of context is the incident, event, or activity that is modeled. They have been grouped into the following categories: *Terrorist Attacks and Other Criminal Activities, Natural Disasters, Transportation Incidents, Industrial and Infrastructure Incidents, Public Events,* and *Routine Security Operations.*

Terrorist Attacks and Other Criminal Activities includes chemical, biological, radiation, nuclear, and explosive (CBRNE) attacks, mass shootings, and cyber crime. *Natural Disasters* includes hurricanes, earthquakes, tornadoes, tsunamis, floods, wildfires, snow, and ice storms. *Transportation Incidents* includes plane crashes, hijackings, train derailments, vehicle crashes, ship board fires and sinking, bridge collapses, and tunnel failures. *Industrial and Infrastructure Incidents* includes chemical spills and other releases of hazardous materials, plant fires and explosions, building collapses, telecommunications system failures, and power blackouts. *Public Events* includes political conventions, inaugurations, protest marches, and rallies; parades; the Super Bowl, Olympics, marathons, and other sporting events; concerts; and other large public events. *Routine Security Operations* includes such as package/baggage screening, security patrols, and surveillance systems for hospitals, courthouses, government agencies, public buildings, seaports, border areas, and airports.

4.3 Emergency Support Functions

In the National Response Framework, DHS defines 15 emergency support functions [17]. The functions define a common set of functions that organizations within and outside of government perform to prepare for and respond to natural disasters, terrorist attacks, industrial accidents, and other incidents. The functions that have currently been defined are *Transportation; Communications; Public Works and Engineering; Firefighting; Emergency Management; Mass Care, Emergency Assistance, Housing and Human Services*; *Logistics Management and Resource Support; Public Health and Medical Services; Search and Rescue; Oil and Hazardous Materials Response; Agriculture and Natural Resources; Energy; Public Safety and Security; Long-Term Community Recovery; and External Affairs.*

Transportation reports damage to transportation infrastructure as a result of an incident; processes and coordinates requests for Federal and civil transportation support; coordinates alternate transportation services, restoration, and recovery of the transportation infrastructure; and coordinates prevention, preparedness, and mitigation among transportation infrastructure stakeholders at the state and local levels. *Communications* provides the required temporary telecommunications and helps restore telecommunications infrastructure. *Public Works and Engineering* conducts pre- and post-incident assessments of public works and infrastructure, executes emergency contract support of life-saving and life-sustaining services, provides technical assistance such as engineering expertise, provides emergency repair of damaged infrastructure, and implements and manages Public Assistance Program and other recovery programs. *Firefighting* focuses on the detection and suppression of wild land, rural, and urban fires and provides personnel, equipment, and supplies in support of the firefighting operations. *Emergency Management* facilitates information flow in the pre-incident prevention, supports and facilitates multi-agency planning and coordination during the post-incident phase. *Mass Care, Emergency Assistance, Housing, and Human Services* provides economic assistance and other services, for individuals, households and families impacted by the incident; the services may include sheltering of victims, organizing feeding operations, providing emergency first aid, providing short- and long-term housing needs, providing victim-related recovery efforts such as counseling, etc. *Logistics Management and Resource Support* provides emergency relief supplies, facility space, office equipment, office supplies, telecommunications, contracting services, transportation services, security services, and personnel for immediate response activities. *Public Health and Medical Services* provides supplemental assistance for the public health and medical needs of victims. *Search and Rescue* provides specialized life-saving assistance including locating, extricating, and providing onsite medical treatment to victims trapped in collapsed structures. *Oil and Hazardous Materials Response* provides the hazard-specific response mechanisms to support actual or potential oil and hazardous materials incidents. *Agriculture and Natural Resources* provides nutrition assistance; animal and plant disease and pest response; safety and security of the commercial food supply; and protection of natural resources, cultural resources, and historic properties. *Energy* is designed to support incident management requirements including force and critical infrastructure protection, security planning and technical assistance, technology support, and public safety in both pre-incident and post-incident situations. *Public Safety and Security* provides a mechanism for coordinating and providing supports that include non-investigative/non-criminal law enforcement, public safety, and security capabilities and resources. *Long-Term Community Recovery* provides a framework for Federal Government support, including Federal's available programs and resources, to enable community recovery from the long-term consequences of the incident and to reduce or eliminate risk from future incidents. *External Affairs* coordinates Federal actions to provide the resource support and mechanisms to Federal, State, local, and tribal incident management elements in order to ensure the required public affairs support or assets are employed.

4.4 Life Cycle Phases

Life cycle phases are major related sets of actions that occur before, during, and after an incident which are designed to minimize its negative consequences, e.g., casualties and property damage. The definitions of life cycle phases are adapted from the DHS National Incident Management System [18]. National Response Framework [19] is replacing the National Response Plan (NRP) [20] in March 2008. It defines response actions as prepare, respond and recover. The five life cycle phases that defined here include *Prevention, Preparedness, Response, Recovery,* and *Mitigation*.

Prevention is defined as the actions that are taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Preparedness includes the range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and private sector and non-governmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

Response is defined as the activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Recovery is defined as the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services. Recovery includes individual, private sector, non-governmental, and public assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration. It also includes evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Mitigation is defined as the activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

5. Implementation Characteristics

The last group of characteristics of the taxonomy focuses on how an MSA application is implemented. The characteristics are representation techniques, interaction modes, human interfaces, data sets, standards, and planning scenarios. Each of these characteristics is described in more detail below:

5.1 Representation Techniques

A number of different representation techniques may be used to describe homeland security area of interest or implement an MSA application as computational systems. The technique chosen will in large part determine how faithfully or accurately a MSA application will represent the real world. Some of the major categories of representations include: *Conceptual Diagrams and Models, Mathematical Models, Dynamic Models, Programming Paradigms, and Analysis Techniques.*

Conceptual Diagrams and Models includes various graphical representations and static models such as influence diagrams, flowcharts, causal loop diagrams, decision trees, and Unified Modeling Language (UML) specifications. *Mathematical Models* includes various equations and formulae, as well as optimization approaches such as linear and integer programming. *Dynamic Models* is used for modeling transformation of a state space over time using representations such as finite state machines, discrete event, continuous, system dynamics, finite element analysis, and computation fluid dynamics. *Programming Paradigms* is to determine how an MSA application will be coded: procedural, agent based, rule based, object oriented, look up tables, data flow, parallel and distributed, neural nets, and cellular automata. *Analysis Techniques* is used for drawing conclusions from the results of implemented models and simulations such as statistical analysis, analytic hierarchy process, weighted ranking, and strategic analysis models.

5.2 Interaction Modes

The DoD has established terminology for characterizing the interaction modes associated with different types of MSA applications, i.e., *Live, Constructive,* and *Virtual. Live* is a simulation involving real people operating real systems. A *Virtual* is a simulation involving real people operating simulated systems. *Virtual* simulations inject human-in-the-loop in a central role by exercising motor control skills (e.g., flying an airplane), decision skills (e.g., committing fire control resources to action), or communication skills (e.g., as members of a command, control, communications, computers, and intelligence team). *Constructive* involves simulated people operating simulated systems. Real people stimulate (make inputs) to such simulations, but are not involved in determining the outcomes. This classification has limitations as identified by DoD itself [6]; however, it can serve as one among many dimensions for the purpose. Game technology provides additional types of interaction modes that are too varied and complex to address within the scope of this document.

5.3 Human Interfaces

Another characteristic of an MSA application is the types of human interfaces it provides. Human interfaces determine who can interact with the application and the types of roles they may play. Categories of interfaces include *Systems Engineering and Support Staff, Instructor and Trainer, System Administrators, Exercise Management, On Scene Response, Response Management, Support Institution Staff, Civilian Population,* and *Opposing Forces*. Many of the interfaces are specific to applications used for training.

Systems Engineering and Support Staff is used to develop, modify and control MSA applications and for executing systems engineering processes. *Instructor and Trainer* is for configuring simulation-based instruction, initiating exercises, controlling flow, interrupting the execution, modifying execution parameters, and tracking student progress. *System Administrators* is used to deal with issues such as installation versions, linking with databases and other systems. *Exercise Management* is used to control the simultaneous execution of multiple MSA applications and interactions with human participants in the exercise. *On Scene Response* allows performing responder roles at an incident site including fire fighting, crowd control, victim triage, and terrorist capture. *Response Management* is used for training of decision makers in incident command center and emergency operations centers at various levels of hierarchy. *Support Institution Staff* is for organizations, such as hospitals, that provide disaster support. *Civilian Population* allows role-playing for civilians caught up in an emergency incident. *Opposing Forces* is used for playing the role of terrorists or enemy combatants unleashing an attack.

5.4 Data Sets

MSA applications need to access many different types of homeland security-related information that originates from various sources. The required information, such as weather, population, terrain, traffic, resources, and infrastructure data may be stored plain text files, structured interchange formats, or remote databases. The format of this data may be based on standards or proprietary formats of information providers. The distribution of timely and accurate information is a key to enhancing the ability to manage all phases of homeland security planning, incident management, routine security operations, and emergency response. This section introduces the classification of data sets that maintain different types of data requirements. Examples of major categories of data sets include *Incidents, Environment, Resources, Controlling Documents, Geography and Layout, Demographic and Behavioral, Investigative Intelligence, Training, Systems Engineering, and Simulation Support.*

Incidents data includes incident summaries, chronologies, response operations, models, message logs, media files, reports and other records, and after action reviews. *Environmental* data includes climate, weather, societal, political, economic, biosphere, and chemical properties/hazard effects data. *Resources* data includes organizations, funds, facilities, personnel, systems, vehicles, other equipment, communications channels, document media, and consumable supplies. *Controlling Documents* data includes policies, plans, protocols, and procedures. *Geography and Layout* data includes definitions of geographical regions and other areas, maps, layouts, and models. *Demographic and Behavioral* data includes demographic and behavioral data. *Investigative Intelligence* include various databases that are mined to gather intelligence for combating terrorism including locations, facilities, organizations, individuals, components, documents, money, weapons, vehicles, and drugs [21]. *Training* data includes course syllabi, lesson plans, instructional materials, tests, exercises, and references. *System Engineering* data includes requirements analyses, design specifications, system documentation, test plans and procedures, and test data sets. *Simulation Support* data includes software assets, statistical distributions, and programming scripts.

5.5 Standards

Standards help the homeland security community make more effective and efficient use of MSA applications. The standards must support the design, development, and implementation of the MSA applications. Examples of major categories of standards that are relevant to MSA applications include *Architectures, General Purpose Integration Interfaces, Domain-specific Integration Interfaces, Equipment Specifications, Operational Guidelines,* and *Document Formats*.

Architectures support the overall design or structure of a system or system environment. Integration interface standards facilitate the interoperation or data exchange between systems. *General Purpose Integration Interfaces* are used to integrate a wide variety of computer applications and are not specific to homeland security or related mission areas. Example interfaces include markup languages, image file formats, and database query languages. *Domain-specific Integration Interfaces* are specific to homeland security related areas, e.g., emergency communications message formats. *Equipment Specifications* define required capabilities, functional characteristics, or rules that ensure quality, safety, and health of users. *Operational Guidelines* define organizational structures, policies, procedures, and protocols. *Document Formats* specify layout and structure for documents in word processing, database, spreadsheet, graphic, presentation, printed and encoded formats.

5.6 Planning Scenarios

This characteristic is used to identify the planning scenarios that the MSA application supports. Planning scenarios may be thought of as specific data sets that are designed to prepare homeland security organizations for a particular type of incident. DHS has defined eight key scenario sets with common characteristics to integrate planning for like events, and to conduct crosscutting capability development. The eight sets are comprised of fifteen national planning scenarios that help focus efforts to prepare for natural disasters, terrorist attacks, and other serious incidents [17]. The national planning scenarios are *Improvised Nuclear Device; Aerosol Anthrax; Pandemic Influenza; Plague; Blister Agent; Toxic Industrial Chemicals; Nerve Agent; Chlorine Tank Explosion; Major Earthquake; Major Hurricane; Radiological Dispersal Device; Improvised Explosive Device; Food Contamination; Foreign Animal Disease;* and *Cyber Attack*.

The *Improvised Nuclear Device* scenario is based upon a 10-kiloton nuclear detonation in a large metropolitan area. The *Aerosol Anthrax* scenario is an aerosol attack spread by a truck in a city. The *Pandemic Influenza* scenario involves the outbreak of influenza for which there has not been an effective preplanned response. The *Plague* scenario is a pneumonic plague that strikes three areas of a major metropolitan city. The *Blister Agent* scenario involves a light aircraft spraying chemical blister agents into a packed college football stadium. The *Toxic Industrial Chemicals* scenario is an attack where a group of terrorists land helicopters at a petroleum refinery, start fires with rocket-propelled grenades and improvised explosive devices that result in a toxic chemical release. In the *Nerve Agent* scenario, Sarin vapor is released into the ventilation systems of three commercial office buildings in a busy metropolitan area. The *Chlorine Tank Explosion* scenario involves an explosion at an industrial facility and the release of a large quantity of chlorine gas. The *Major Earthquake* is a 7.2 magnitude quake that occurs along a fault zone in a major city. The *Major Hurricane* scenario describes a Category 5 hurricane that hits a major metropolitan area. The *Radiological Dispersal Device (RDD)* scenario involves separate Cesium Chloride bomb attacks on three regionally close, moderate-to-large cities. The *Improvised Explosive Device* (IED) scenario involves IED bombings inside a sports arena, at a parking facility near an entertainment complex, and suicide bomber attacks in an underground public transportation concourse. The *Food Contamination* scenario involves the distribution of anthrax-contaminated ground beef and orange juice to different states and cities. The *Foreign Animal Disease* scenario is a coordinated bio-terrorism attack that infects farm animals with foot and mouth disease at several large livestock operations. The *Cyber Attack* is a computer attack that is directed at several parts of the national financial infrastructure over the course of several weeks.

6. Conclusions and Next Steps

This paper has provided an overview of a proposed taxonomy for classifying homeland security MSA applications. The major categories of the classification scheme are application objectives, target organizations and missions, simulation contexts, and implementation characteristics. A more comprehensive technical report is under development that specifies each category in greater detail. External review workshops are planned in 2008 to obtain expert feedback from the homeland security community on the taxonomy. Future work will focus on identifying and establishing a database of existing MSA applications, identifying best practices found in existing applications, developing needs and requirements analyses for future MSA applications, identifying existing standards and gaps that need to be filled to support MSA applications.

References

[1] S. Jain and C. R. McLean: “Modeling and Simulation of Emergency Response: Workshop Report, Relevant Standards and Tools” National Institute of Standards and Technology Internal Report-7071, 2003.

[2] National Science Foundation (NSF): Simulation-Based Engineering Science, 2006, Available on line via: < http://www.nsf.gov/pubs/reports/sbes_final_report.pdf >.

[3] National Research Council: Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Academies Press, Washington DC 2002.

[4] J. Banks (Ed.): Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice, John Wiley, New York, 1998.

[5] Department of Defense: DoD Modeling and Simulation (M&S) Management, DoD Directive 5000.59,1994.

[6] Department of Defense: Modeling and Simulation Master Plan, DoD 5000.59-P, 1995.

[7] US Navy: M&S Educational Training Tool (MSETT), Navy Air Weapons Center Training Systems Division Glossary, 1994.

[8] Cambridge University: Cambridge index of modeling and analysis tools, Cambridge University, Institute of Manufacturing, 2008. Available online via: < http://www.ifm.eng.cam.ac.uk/dstools/>.

[9] Department of Defense: Systems Engineering Fundamentals, Defense Acquisition University Press, Fort Belvoir, Virginia 2001. Available on line via: < http://www.dau.mil/pubs/pdf/SEFGuide%2001-01.pdf>.

[10] http://en.wikipedia.org/wiki/Linnaean_taxonomy

[11] http://en.wikipedia.org/wiki/Categorization

[12] W. Zachary: “A Cognitively-Based Functional Taxonomy of Decision Support Techniques”ACM

SIGCHI Bulletin, Vol. 19, Iss.1, pp: 72 – 73, July 1987.

[13] Department of Homeland Security: Homeland Security Presidential Directive 8 Annex 1, 2007. Available on line via: <http://www.dhs.gov/xabout/laws/gc_1199894121015.shtm>.

[14] B. S. Bloom: Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain, David McKay, New York 1956.

[15] S. Jain and C. R. McLean: “An Integrating Framework for Modeling and Simulation for Incident Management” Journal of Homeland Security and Emergency Management, Vol. 3, No. 1, Article 9, 2006.

[16] S. Jain and C. R. McLean: “An Integrated Gaming and Simulation Architecture for Incident Management Training” National Institute of Standards and Technology Internal Report NISTIR-7295, 2006.

[17] Department of Homeland Security: National Response Plan, 2004. Available on line via: <http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf>.

[18] Federal Emergency Management Agency (FEMA): Drift Revised NIMS Document, 2007. Available on line via <http://www.fema.gov/emergency/nims/nims_doc.shtm>.

[19] Federal Emergency Management Agency (FEMA): National Response Framework, 2008. Available on line via: <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

[20] Department of Homeland Security: Notice of Change to the National Response Plan, 2006. Available on line via: <http://www.dhs.gov/xlibrary/assets/NRP_Notice_of_Change_5-22-06.pdf>.

[21] J. Mena: Homeland Security - Techniques and Technologies, 2004. Charles River Media, Hingham, MA 2004.

Acknowledgement and Disclaimer

The Science and Technology Directorate of the Department of Homeland Security (DHS) and the Manufacturing Systems Integration Division of the National Institute of Standards and Technology (NIST) sponsored work described in this report. The work described was funded by the United States Government and is not subject to copyright.

Author Biographies

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, the Editorial Boards of the International Journal of Production, Planning, and Control, the Journal of Simulation, and the Journal of Digital Enterprise Technology. He is Secretary of the Crisis Management and Societal Security Forum within the Simulation Interoperability Standards Organization (SISO). 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 a Masters of Science in Information Engineering from University of Illinois at Chicago and a Bachelor of Arts from Cornell University, Ithaca, NY.

SANJAY JAIN is an Assistant Professor in the Department of Decision Sciences, School of Business at the George Washington University (GWU). His research is sponsored by the National Institute of Standards and Technology. Sanjay serves as an associate editor of the International Journal of Simulation and Process Modeling and also as a member of the editorial board of International Journal of Industrial Engineering. He is a senior member of the Institute of Industrial Engineers and a member of APICS - The Association for Operations Management. He received a Bachelors of Engineering from Indian Institute of Technology (IIT)-Roorkee, India, a Post Graduate Diploma from National Institute of Industrial Engineering, Mumbai, India, and a Ph.D. in Engineering Science from Rensselaer Polytechnic Institute, Troy, New York.

Y. TINA LEE is a computer scientist of the Manufacturing Engineering Laboratory at the National Institute of Standards and Technology (NIST). She joined NIST in 1986. Her major responsibility in recent years is to develop information models to support various manufacturing application areas. She is a member of ISA and Simulation Interoperability Standards Organization (SISO). She is currently secretary of SISO's Core Manufacturing Simulation Data Product Development Group. Prior to NIST, she worked at the Contel Federal Systems, Sperry, and Research & Data Systems. She received her BS in Mathematics from Providence College and MS in Applied Science from the College of William and Mary.