Decision Support for Campus Emergency Response Management

Amine Chigani
Department of Computer Science
Virginia Polytechnic Institute and State University (Virginia Tech)
Blacksburg, VA 24061, U.S.A.
achigani@vt.edu
+1 (540) 231-7542

Osman Balci
Department of Computer Science
Virginia Polytechnic Institute and State University (Virginia Tech)
Blacksburg, VA 24061, U.S.A.
balci@vt.edu
+1 (540) 231-4841

Reza Barkhi *
Department of Accounting and Information Systems
Virginia Polytechnic Institute and State University (Virginia Tech)
Blacksburg, VA 24061, U.S.A.
Barkhi@vt.edu
+1 (540) 231-5869

April 5, 2011

* Corresponding Author

ABSTRACT

The history of university, college, and high school campuses is eventful with man-made tragedies ensuing a tremendous loss of life and property. Virginia Tech's April 16 tragedy ignited the discussion about balancing openness and safety in open campus environments. Decision makers in educational institutions face the challenge of ensuring that their campuses provide an open learning environment and at the same time are safe. Most deployed technology solutions are characterized by addressing bits and pieces of the problem (e.g. electronic notification systems). Without a comprehensive understanding of the requirements for an institution-wide solution that facilitates augmented situational awareness and efficient emergency response, the proposed solutions fall short of the desired outcome. This paper provides a capabilities specification for such a solution. The capabilities specification serves as a case study and a framework that guide the architecting, design, and implementation of decision support systems that facilitate campus emergency response management.

Keywords: Capabilities specification; Design science framework; Emergency response management; Situational awareness; Campus security control; Decision support

1. INTRODUCTION

Academic institutions operating in open campuses are facing an increasing challenge to protect their constituents while maintaining the open nature of their campuses. A major aspect of this challenge is enabling administrators and first responders anticipate as well as respond effectively to incidents. On April 16, 2007, Virginia Tech was a scene for the most tragic shootings in American school history leaving 32 students and faculty dead and 17 others wounded [16]. In the wake of this tragedy, several issues were identified regarding the ability of schools to maintain a balance between safety and openness. To study the events leading to this incident, a panel called the Virginia Tech Review Panel was convened, the purpose of which was to investigate and to assess the effectiveness of the response by decision makers and public safety entities during and after the incident.

Notably, a key finding of the Virginia Tech Review Panel was that "the university did not respond effectively" in spite of the fact that various individuals and entities within and outside the university knew pieces of relevant information. The panel cites, however, that the reason for this failure is that "no one knew all the information and no one connected all the dots" [17]. In other words, the study blames the failure on a lack of a decision support mechanism that would have enabled decision makers to *connect the dots*. The unfortunate April 16 tragedy presents a clear case for the need for an integrated decision support system that enables groups of decision makers to "connect the dots" through interoperable communication and information sharing facilities of a Group Decision Support System (GDSS). This finding is supported by other studies that dealt with emergency response management to man-made disasters [9].

A GDSS plays a critical role in the success of an organization and provides essential support to the decision-making process at all levels, including planning, operations, and management [15]. Nevertheless, the acquisition influx of an electronic notification system (ENS) by educational institutions in the aftermath of Virginia Tech's shootings reflects a typical reaction to solve a multi-faceted problem by using off-the-shelf, one-size-fits-all technology. Unfortunately, available technologies, such as ENS, provide only bits and pieces of the desired solution. Addressing this issue needs to consider many technical, legal, and social aspects. In this paper, we address this need by examining the role of software-based technology in establishing a safe campus environment through the integration of disparate information systems, databases, departments, and agencies around campus.

This study is a part of a larger research project, which proposes to develop a service-oriented architecture for a GDSS called SINERGY: campu**S** s**I**tuational aware**N**ess and **E**mergency **R**esponse mana**G**ement s**Y**stem. SINERGY is a software-based, network-centric system of systems intended to provide situational awareness, security control, and emergency response management for open campus environments. To accomplish this, the project is structured into four phases: Problem formulation, capabilities specification, architecture specification, and architecture evaluation. In this paper, we report on the first two phases of the research, which consisted of a study we conducted within the Virginia Tech campus to perform a domain analysis about a GDSS that supports emergency response management for open campus environments. We define the problem and propose a capabilities specification of the GDSS based on interviews that we conducted with the stakeholders so that the system capabilities reflect the user requirements.

The results of the study contribute to the design science of GDSS [5]. Design science is concerned with creating various life cycle artifacts of a system under development [14]. Artifacts of design science are of four categories: constructs, models, methods, and implementations [13]. This paper presents a system capabilities specification – a contribution that falls under the category of constructs. Constructs form a set of concepts that enables developers to analyze, characterize, and communicate about a system context. The capabilities specification presented herein provides a framework for a GDSS that supports campus emergency response management and serves as an input to the architecting and design of such systems. This framework describes *key capabilities* and *quality attributes* that should be present in any GDSS for campus emergency response management. Hence, the framework guides the future development of various types of GDSS for campus emergency response management.

The remainder of this paper is organized as follows. Section 2 presents the research approach. Section 3 describes the types of stakeholders of SINERGY. Section 4 describes stakeholders' functionality needs along with the SINERGY capabilities that satisfy those needs. Section 5 describes SINERGY quality attributes and Section 6 lists the intended uses of SINERGY. Finally, we present our concluding remarks in Section 7.

2. RESEARCH APPROACH

Figure 1 shows the four phases of our research and the first two phases that are the focus of this paper. The ultimate goal of this work is to develop an architecture for a GDSS that will facilitate coordinated decision making and address the issue of balancing safety and openness for campuses. To do so, however, we need to understand what it is that we plan to architect. For this purpose, we need to formulate the problem concisely taking into consideration social and legal constraints, and elicit the functional and quality needs that will guide the architecting process. Therefore, our approach consists primarily of: 1) involving campus constituents including students, staff, administrators, law enforcement, and first responders in specifying the desired solution; 2) studying the characteristics of open campuses and the legal guidelines that govern them; 3) surveying the technologies that best support the achievement of the desired solution; and 4) deriving and specifying functional and quality requirements that guide the architecting, design, and development of such a system.

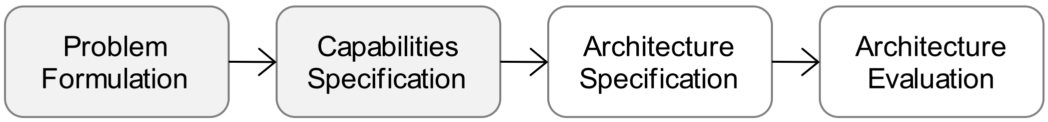

Figure 1: Phases of our research

2.1. Problem Formulation

What it means to be safe in an open campus differs from one institution to another, from one administrator to another, and from one law enforcement agency to another. However, commonalities exist across these differences. Figure 2 illustrates how we formulate the problem of campus safety based on our comprehensive study of the Virginia Tech campus environment. We view this problem from three complimentary prisms: situational awareness, security control, and emergency response management. In other words, a safe and open campus environment can be realized through a GDSS that enables the creation of a common operating picture (COP) of the campus environment shared by all campus entities (i.e., situational awareness). Having a COP of what goes on campus at any point in time is key for law enforcement personnel to put in place effective security control measures in real-time decision-making context [3]. Finally, common situational awareness and deliberate security control lay the foundation for an efficient and effective emergency response in the case of an emergency.

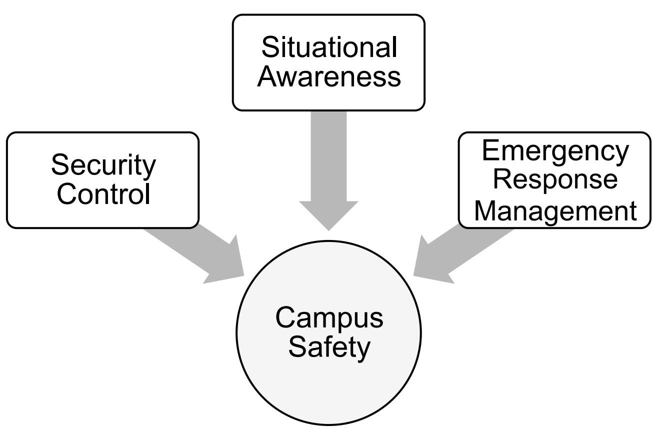

Figure 2: Elements of safety in open campuses

2.2. Capabilities Specification

We elicit SINERGY capabilities by interviewing stakeholders who have expertise regarding campus safety and find initiatives to campus safety as critical. Virginia Tech's resources (students, staff, faculty, campus structure, and existing systems) provided the context for these interviews. The context of the study helped us focus on understanding the problem domain and deriving *key capabilities* and *quality attributes*. Figure 3 illustrates the process through which the capabilities and quality attributes were identified. In addition, this phase was guided by the opinions of subject matter experts (SMEs) in related technologies and research areas. Finally, our study was complimented by participating in the Incident Command System (ICS) training program offered by the Federal Emergency Management Agency (FEMA) Emergency Management Institute [11]. This program provided us with the understanding of best practices in emergency management, and the legal constraints that guide these practices. Our objective was to conceptualize practice to guide GDSS design for campus safety, so that the systems facilitate coordination and response in a real-time decision-making context that characterize emergency response situations.

Figure 3: Elicitation process of capabilities and quality attributes

Table 1 shows a list of SINERGY stakeholder categories. We interviewed a number of representatives from each of the categories listed as indicated by the number next to the stakeholder category. The interviews focused on the capabilities that SINERGY should provide as a potential solution to current security and emergency management challenges from their perspective.

Table 1: List of stakeholder categories

Stakeholder Category	Examples
Administrators (4)	University president, vice president, dean, department chair
Campus Constituents (34)	Faculty, staff, students, campus visitors
Security Providers (6)	University police, town police, residence hall directors/assistants
First Responders (7)	Firefighters, hospital staff, university emergency staff, health center staff
Subject Matter Experts (11)	Wireless sensor network researchers, autonomous systems researchers, information management researchers, social media researchers, sociologists

2.3. Assumptions and Constraints

Although the capabilities and quality attributes described in this paper can be generalized to any GDSS that supports emergency response management, the research is conducted under certain assumptions and constraints that represent state-of-art technologies and clear standards. First, SINERGY shall be based on the service-oriented architecture (SOA) using web services technology. Second, SINERGY architecture shall be represented by using the Department of Defense Architecture Framework (DoDAF) Version 2.0 [6,7,8]. Third, SINERGY architecture shall represent a "to-be" viewpoint of the system, i.e., a desired system to be built. Finally, the campus police department shall establish a dedicated SINERGY command center to manage its resources and serve as the command center for emergency response efforts. This link from decision to action is critical given the GDSS real-time decision context and the importance of real-time action as a proper response to each incident.

2.4. Types of Emergencies

Based on the interviews with 62 stakeholders, we identified the scope of incidents for which SINERGY should be designed. In order to focus our study on the types of emergencies that may effect campus environments, we consider those emergencies that may result in potential threats to the life of those on campus. Figure 4 shows a toxonomy of the types of incidents for which SINERGY may be employed.

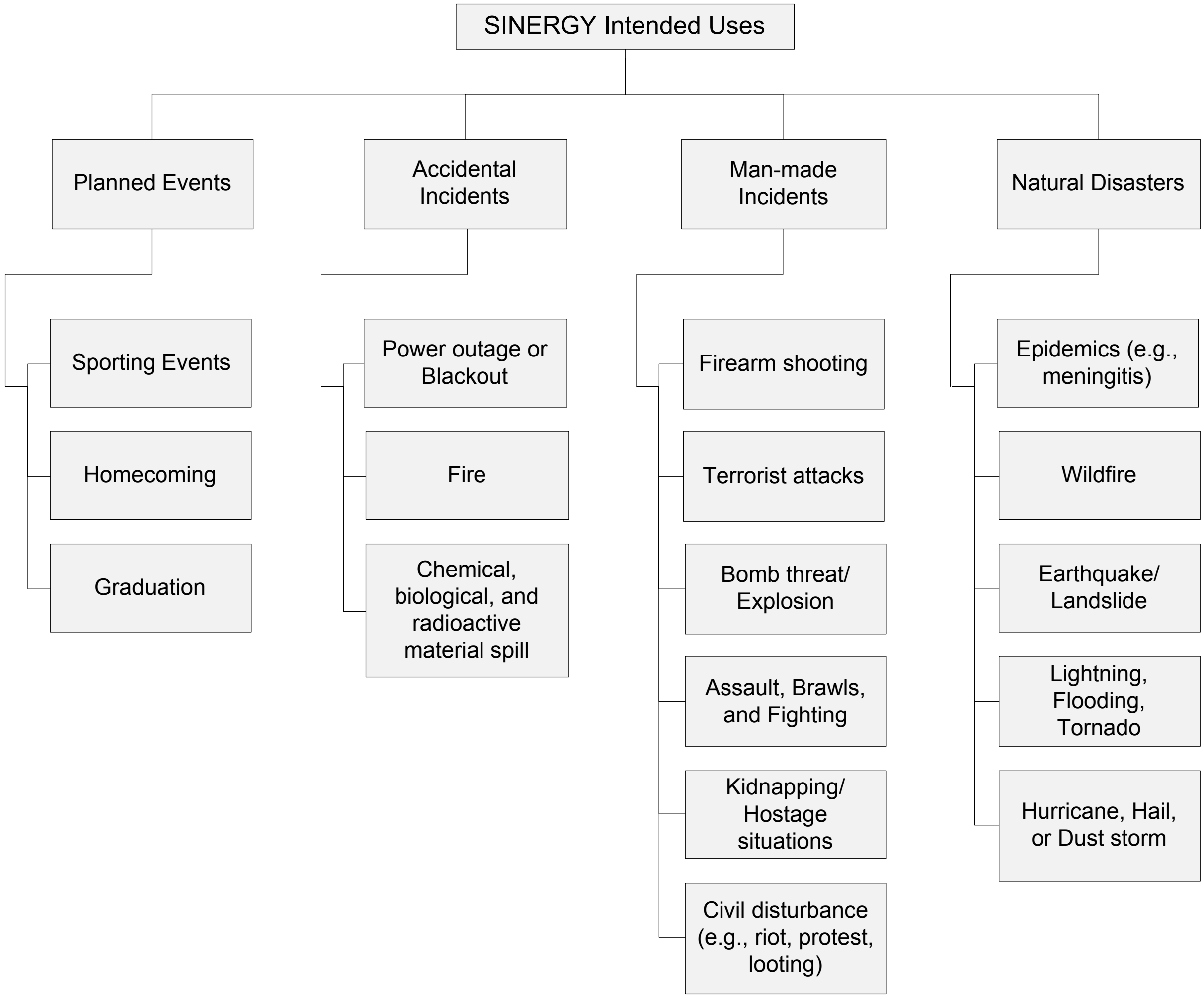

Figure 4: Types of incidents for which SINERGY can be used

3. STAKEHOLDER TYPES

Stakeholder analysis is essential to ensuring the relevance of any proposed solution. In this study, we identified several stakeholders who are likely to impact and be impacted by SINERGY. We classified these stakeholders into *passive* and *active* stakeholders.

3.1. Passive Stakeholders

Passive stakeholders are those who will not interact or use the system directly or actively once the system is operational. However, these stakeholders have a lot of input and interest (stake) in the system and they influence what quality characteristics the system should possess. This category of stakeholders includes sponsors and subject matter experts (SMEs).

For SINERGY, Table 2 lists the passive stakeholders from which we received input.

Table 2: List of SINERGY passive stakeholders

Researchers in the Digital Libraries for Crisis, Tragedy, and Recovery Research Network, Department of Computer Science, Virginia Tech
Researchers in the Cultural Differences in Emergency Response, Department of Sociology, Virginia Tech
Researchers in the Use of Phones and Social Networks during Emergencies, Department of Accounting and Information Systems, Virginia Tech
Office director of Converged Technologies for Security, Safety, and Resilience, Virginia Tech
Medical doctors and administrator of the Schiffert Health Center, Virginia Tech
Researchers and administrator of the Emergency Planning in Biological and Chemical Research, Via College of Osteopathic Medicine (VCOM), Virginia Tech
Autonomous systems researcher, Institute of Critical Thinking & Applied Science, Virginia Tech
System architect from Communications Network Services, Alerts Systems, Virginia Tech
Experts in campus security, Q&A webinars organized by Campus Technology [4]

3.2. Active Stakeholders

Active stakeholders, on the other hand, are those who will actively and directly interact and use the GDSS once it becomes operational. Examples of these stakeholders include faculty, students, campus administrators, campus security, and law enforcement personnel.

For SINERGY, Table 3 lists the active stakeholders who participated in the interviews.

Table 3: List of SINERGY active stakeholders

Director of the Office of Emergency Management, Virginia Tech
Director and staff of the Office of Residential Life, Virginia Tech
Officer from the Virginia Tech Police Department, Crime Prevention Unit and Outreach
Vice president of University Relations, President's Office, Virginia Tech
Officers from the Blacksburg Police Department, Blacksburg, VA
Students from Virginia Tech campus: full-time, part-time, undergraduate, graduate, on-campus, off-campus, Blacksburg campus, and extended campus

The list of stakeholders shows the diversity of individuals, groups, and entities that hold a stake in SINERGY. Given that a GDSS is designed for a multi-participant, multi-objective, and multi-criteria decision problem, adhering to these inputs is critical. Given the importance of these inputs, we elaborate on the functionality and quality needs of each stakeholder type that we derived from the interviews.

4. FUNCTIONALITY NEEDS: CAPABILITIES

Educational institutions, as any large enterprise, must comply with state and federal regulations in the preparation for emergencies and establishment of contingency plans for responding to threats that could harm personnel, faculty, students, and/or property. They are required to establish an Emergency Management office that works in tandem with other university offices to create response plans to emergencies not only for the short term but also for the long term. The director of this office serves as the campus emergency response manager in case of an incident involving the university.

Educational institutions should also comply with the Incident Command System (ICS), which is FEMA's recommended emergency management framework that guides response plans to emergencies [11]. Within this system, the director of the Emergency Management office serves as the Incident Commander (IC) and is responsible for assembling and managing all the agencies that need to collaborate in response to an incident.

Based on the interviews conducted with SINERGY stakeholders, a list of functionality needs have been identified. These functionality needs are specified in terms of capabilities. A capability is a broader concept than a requirement, and refers to what a system provides but will not elaborate on the details of how it is provided. Formally, a *capability* is defined as "the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks" [7, p. 80].

Table 4 lists stakeholders' functionality needs. This list covers the overarching needs expressed by more than one stakeholder. The list represents a starting point for the identification of SINERGY capabilities and the SOA architecture facilitates expending functionalities to build on the initial design. Each need represents a high-level specification of a capability or a set of capabilities that the stakeholders would like SINERGY to provide. These needs are grouped by the three components of SINERGY's overall goal: security control, situational awareness, and emergency response management.

Table 4: List of stakeholders' functionality needs

Security Control
Diverse incident detection capabilities
Diverse incident reporting capabilities
On-demand surveillance capabilities
Situational Awareness
Common operational picture capabilities
Geographical Information System and campus visualization capabilities
Audible situational awareness capabilities
Visual situational awareness capabilities
Electronic text situational awareness capabilities
Emergency Response Management
Direct communication with emergency response personnel capabilities
Response coordination capabilities
Documentation capabilities for decisions, expenses, and damages
Training capabilities for personnel and public

4.1. Diverse Incident Detection Capabilities

One of the major needs, as stated by several law enforcement personnel, from a system such as SINERGY is to "*help them anticipate incidents before they happen and detect them as they unfold.*" Diverse detection capabilities are essential to enabling security control personnel do their jobs effectively.

> **Capability Statement:** SINERGY shall provide the capability of managing a video-based surveillance network consisting of multiple cameras deployed across campus, operated by the campus police department.

> **Capability Statement:** SINERGY shall provide the capability of managing a network of sensors deployed around critical infrastructure facilities on campus, operated by managers of those facilities.

> **Capability Statement:** SINERGY shall provide analysis capabilities of recorded and sensed data to detect security warnings and anticipate incidents before they occur. Security experts within campus law enforcement shall manage these capabilities.

4.2. Diverse Incident Reporting Capabilities

SINERGY is expected to enable the reporting of incidents to security personnel. Diverse reporting capabilities are needed to enable both security providers and campus constituents "*share the responsibilities of making the campus safe*" by reporting incidents in a variety of ways.

Capability Statement: SINERGY shall provide students, faculty, and staff the capability to report incidents to an established SINERGY command center through the following means:

- Fax: a dedicated incident report fax number
- 911 Dispatch: cellular phone, landline phone, and VoIP (Voice-over-IP) applications
- E-mail: a dedicated incident reporting e-mail address that accepts e-mails with documents, photos, and videos as attachments
- Messaging: a dedicated number that accepts SMS (Short Message Service) and MMS (Multimedia Messaging Service) messages
- Online, location-based, and secure incident reporting portal
- Mobile, location-based, and secure incident reporting software application for mobile devices

Capability Statement: SINERGY shall provide law enforcement personnel the capability to report incidents to the command center through the means mentioned above in addition to:

- Police in-car computers
- Two-way radios (walkie-talkies)

4.3. On-demand Surveillance Capabilities

On-demand surveillance is important due to privacy concerns in campus environments. Locker rooms, classrooms, dining rooms, residential halls, and athletic facilities "*are personal areas and cannot be monitored all the time.*" However, during an emergency, it is critical that these areas are monitored to manage the response to an incident. Need-based surveillance is a solution to balancing safety and privacy.

Capability Statement: The network of surveillance cameras shall be sensor-based. Sensor-based cameras shall record data only when it detects motion of certain types of objects (e.g., human or animal).

Capability Statement: The network of surveillance cameras shall be IP-addressable. SINERGY shall provide the capability to remotely-manage (switch on and off) these cameras to record only on a need-basis (e.g., during an emergency or at nights).

Capability Statement: SINERGY shall provide the capability to seamlessly integrate a set of newly deployed cameras at the scene of an incident. Law enforcement personnel shall be able to deploy portable surveillance cameras at the scene of an incident and register them into SINERGY to be part of the network of surveillance cameras.

4.4. Common Operational Picture Capabilities

A common operational picture (COP) is a consistent and accurate representation of the overall information to all constituents on campus. The role of Emergency Management director is "*to ensure that the most accurate picture possible of the campus is available to support the decisions of its constituents.*" To do so, an on-demand, interactive, graphical representation of the COP is needed for different SINERGY users personalized to their security roles, responsibilities, and required action responses. This will help each user to receive personalized information corresponding to their decision and action domains.

Capability Statement: SINERGY shall provide a COP for a user's personalized decision-making domain.

Capability Statement: The COP shall be accessible to users based on their access privileges. Capabilities required to generate the COP shall depend on the type of users and their access levels.

Capability Statement: The COP shall be based on the integration of information retrieved from various databases and data services on and off campus including: Student records information, police records, health records, maps and geographical information system (GIS) services, building schematics, and digitized campus maps.

Capability Statement: The COP shall have default instantiations, which shall be recomposable by the user based on user's specified parameters and preferences. For instance, the police shall be able to identify all cameras deployed on campus and activate them to locate a perpetrator or monitor a situation. Administrators shall be able to monitor campus walkways to direct traffic. Health officials shall be able to locate patients' residence and classrooms to reason about the contagiousness patterns of a particular virus.

4.5. GIS and Campus Visualization Capabilities

GIS is a critical enabler of situational awareness. Interviews with a building maintenance manager expressed a need for such capability to help the sharing of consistent and up-to-date building information among different offices on campus.

> **Capability Statement:** SINERGY shall use GIS technology to provide a centralized campus basemap allowing users to download, query, and edit content with proper access privileges.

For instance, the police can have access to the basemap including data about crime statistics, potential hideouts, and risk areas, to anticipate the next move of a loose shooter on campus. The campus health center can place current cases of flu-infected students on the basemap and draw conclusions on possible modes of transmission of this virus on campus. This capability will facilitate more timely responses to incidents.

> **Capability Statement:** SINERGY shall provide visualization capabilities of the COP through the use of large displays, multi-displays, and touch-displays.

4.6. Audible Situational Awareness Capabilities

Audible situational awareness allows campus constituents to know about ongoing incidents through audio technologies. SINERGY shall incorporate audio mechanisms to keep students, staff, and faculty informed about ongoing incidents.

> **Capability Statement:** SINERGY shall provide audible notifications about campus events to all constituents through one or more of the following mechanisms:
>
> - Loudspeakers
> - Sirens
> - Voicemail
> - Fire alarm speaker system
> - Text-to-speech (TTS) tools

4.7. Visual Situational Awareness Capabilities

Visual situational awareness allows campus constituents to know about ongoing incidents through visual technologies. SINERGY shall incorporate visual mechanisms to keep students, staff, and faculty informed about ongoing incidents.

> **Capability Statement:** SINERGY shall provide visual notifications about campus events to all constituents through one or more of the following mechanisms:

- Digital Signage
- In-class digital boards
- Siren lights
- Fire alarm system lights

4.8. Electronic Text Situational Awareness Capabilities

Electronic text (E-text) situational awareness allows campus constituents to know about ongoing incidents through electronic text technologies. SINERGY shall incorporate electronic text mechanisms to keep students, staff, and faculty informed about what is going on campus.

Capability Statement: SINERGY shall provide electronic text reports about campus events to all constituents through one or more of the following mechanisms:

- Webpage updates
- Digital signage
- Desktop alerts software application
- Alerts software applications for mobile devices
- Text messages
- Instant messages
- Twitter updates
- Facebook updates
- Speech-to-Text tools

4.9. Direct Communication with Emergency Response Personnel Capabilities

Communication between SINERGY command center and emergency response personnel is critical. It should be conducted in a direct manner to ensure efficient response efforts. In addition, communication through diverse media ensures that there is always a link between the command center and personnel on the ground.

Capability Statement: SINERGY shall provide direct communication capabilities between incident command and emergency response personnel through one or more of the following means:

- Cellular phones: video and voice
- Satellite-based phones
- VoIP applications: video and voice

- Fax
- Closed instant messages (IM) sessions
- Messages: SMS and MMS
- E-mail
- Two-way radios (walkie-talkies or handheld transceivers)
- Twitter updates

4.10. Response Coordination Capabilities

Coordination is critical to effective and efficient emergency response management. First responders and decision makers need the capability to make, change, and revise decisions based on new information in an efficient manner. Voice and video conference tools are important for providing this capability.

> **Capability Statement:** SINERGY shall provide the capability to create, manage, and moderate voice conferencing sessions where users participate using cell phones, landline phones, or VoIP applications.

> **Capability Statement:** SINERGY shall provide the capability to create, manage, and moderate video conferencing sessions where users participate using camera-equipped devices connected to the Internet.

4.11. Documentation Capabilities for Decisions, Expenses, and Damages

Emergencies and other unanticipated incidents always bring new insights into how the response to them can be more effective. Therefore, learning from such insights and proper updates of documentation of emergency response is critical.

In addition, emergency response managers must keep track of the cost incurred during an incident for accountability, assessment, and insurance claims. For instance, as emergency personnel inspect damages to people, property, and equipment, SINERGY should provide capabilities to store recorded notes, written notes, photos, and videos of the damages.

> **Capability Statement:** SINERGY shall provide the capability to document all operations and transactions that it automatically executes, as well as those operations and transactions the users execute.

> **Capability Statement:** SINERGY shall provide the capability of managing mobile services that

integrate with portable mobile devices (e.g., phones, cameras, netbooks, tablets) to record video, audio, and text information about actions, decisions, and expenses related to emergency response.

4.12. Training Capabilities for Personnel and Public

Security control and emergency response management involves everyone on campus. The ability to train personnel and engage the public is critical. The system should provide access to information about emergency plans, situational awareness resources, security help, and online tutorials. In addition, the system should provide tools to train new personnel about the capabilities and deployed services, and run interactive simulations based on past documented cases for training purposes.

Law enforcement, health care providers, building managers, and others face the challenge of ensuring that each member of their personnel works in tandem with others. This becomes a challenge in the case of new personnel who need to be trained on how to use the capabilities of the system while interoperating with others. The system should facilitate new personnel by going through interactive simulations where they receive proper feedback on their decisions and actions. In addition, administrators expressed the need to be able to inform their staff and the students about the security control measures put in place and the security management plan. Having an online help and training capability that is accessible to them will enable self-paced learning.

> **Capability Statement:** SINERGY shall provide training resources as an online capability to train new personal and to educate students, faculty, and staff about emergency management and security control on campus.

5. QUALITY NEEDS: QUALITY ATTRIBUTES

Quality attributes of a system are those characteristics that affect the quality of the entire system. They are also referred to as quality characteristics and non-functional requirements. Examples include security, interoperability, and performance.

Table 5 lists the quality needs that SINERGY should satisfy, as expressed by stakeholders, in order to support their business goals. These needs are expressed in the language of the problem domain. From this list, we extract key quality attributes for GDSS that support emergency response management in open campus environments.

Table 5: List of stakeholders' quality needs

Quality Need Description
Balance between information control and response flexibility
Interoperability among personnel and among system components
Real-time availability of information
Infrastructure availability during incidents
Fault tolerance and graceful degradation of system performance during incidents
Simplicity of solution to cater to users with limited technical skills

5.1. Balance between Information Control and Response Flexibility

Control over the dissemination of information is critical during emergencies. Decision makers have to walk a fine line between keeping the public informed and avoiding misinformation, secondary incidents, and misuse of information by perpetrators. While lack of information causes problems, too much information can also result in information overload where important messages can be ignored. Meaningful judgments of the tradeoff are crucial. Law enforcement and public relations stakeholders need the capability to control the flow of official information on all SINERGY outlets. Given that new and unanticipated incidents may occur, the flexibility of an emergency response plan is critical. The ability to keep campus constituents informed is important to emergency managers. Providing multiple modes of communication helps in this regard but creates a challenge for controlling which and when information is shared. The GDSS can provide a multi-participant ranking mechanism so that depending on the importance and relevance of the information, it can be shared or not, and on one or multiple communication modes with proper levels of redundancy, speed, and reach.

Security: SINERGY shall allow authorized users to control and manage the dissemination of official information to campus constituents through university official channels (e.g., website, alerts, digital signs, e-mails, twitter updates, and facebook updates.)

Response Flexibility: SINERGY shall provide the capability to disseminate official information to all campus constituents through one or all communication outlets based on the situation to achieve maximum reach and flexibility of the response.

5.2. Interoperability among Personnel and among System Components

Security control and emergency preparedness and response involve many entities within an open campus. The terminology/jargon used by each of these entities is often different. Bringing all these groups to work together raises a communication challenge among individuals from different disciplines such as police officers, medical doctors, administrators, and firefighters. Unifying the communication terminology among these entities becomes a critical aspect of the success of any collaborative emergency response effort. For example, the conciseness of symbolic language and the lack of ambiguity relative to natural language can reduce ambiguity and equivocality in communication. For example, a fire siren is a clear and unambiguous message resulting in an unequivocal action of exiting the building. Similarly, the "check out" button on online stores such as Amazon.com is unambiguous symbolic message from the user to the system indicating that the user wants to act unequivocally by checking out and paying for the purchased items. While symbolic languages enjoy efficiency in communication due to avoiding ambiguity and equivocality, the potential range of incidents should also allow a flexible communication structure. A mix of symbolic language and natural language may be a reasonable tradeoff. In addition, the need to interface with other systems requires adherence to standard architectures to facilitate interoperability.

Interoperability: SINERGY shall be interoperable on three levels.

1. *Terminology:* SINERGY shall be compliant with the Incident Command System (ICS), which advocates a common terminology defining organizational functions, facilities, resource description, and position titles.
2. *Interfaces:* SINERGY shall use web services standards to provide interoperable interfaces among system components, and wrappers for legacy systems.
3. *Data:* SINERGY architecture shall be based on a Service-Oriented Architecture, which prescribes an Enterprise Service Bus (ESB) layer that provides seamless transformation of data shared among services.

Compliance with Standards: SINERGY shall comply with the required technology, legal, and institutional standards.

5.3. Real-time Availability of Information

The need to access information in real-time during an incident is important, especially for campus constituents [12]. Sharing a COP with the public has advantages and disadvantages. Emergency managers believe that "*while sharing of information as it becomes available is desirable, verifying it may take* *time.*" Misinformation can lead to panic or secondary incidents—those resulted as a reaction to a primary incident. In addition, too much information can result in information overload where individuals can potentially disregard critical information when they reach their information processing capacity.

Information Availability: SINERGY shall provide real-time access to information in a pervasive manner through two complimentary mechanisms: 1) push mechanisms such as brief SMS alerts pushed to campus constituents wherever they are, and 2) pull mechanisms such as website updates where the information is updated regularly but constituents need to go to the website and read (pull) it.

5.4. Infrastructure Availability during Incidents

One of the stakeholders stated that "*even the best infrastructure in the world is useless if it is not available when needed.*" An emergency could be that the infrastructure itself failed. Therefore, many stakeholders expressed a need that the emergency infrastructure should be independent from normal operation infrastructure. For instance, an alert system should use servers that are dedicated for this service and does not share resources with other university operations such as e-mails and course management systems. There should also be enough redundancy and decentralized and networked structure so that the breakdown of one node will not bring down the system.

Infrastructure Availability: SINERGY infrastructure shall be available 24 hours a day, 7 days a week. This quality attribute shall be achieved in the following manner:

- SINERGY shall use dedicated physical resources hosted on-site.
- SINERGY shall use redundant physical resources hosted in national and international off-site locations to ensure the availability of capabilities when campus infrastructure is compromised.
- SINERGY command center critical facilities shall be duplicated on a mobile vehicle that can be moved closer or away from an emergency scene as needed.

5.5. Fault Tolerance and Graceful Degradation of Performance during Incidents

Many stakeholders expressed their concerns about the dependencies among deployed technology solutions. When one part of the solution is affected, the entire system goes down. Therefore, the separation of concerns is a key driver for identifying SINERGY capabilities. If e-mail communication is affected due to hardware failure, texting and phone communication should not be affected.

Fault Tolerance: SINERGY shall be fault tolerant and resilient to failure through the adoption of the architecture and design concepts that promote minimal dependencies among system hardware components and among system software components, graceful degradation of performance during failures, and robust response to errors, attacks, failures, and exceptions.

5.6. Simplicity of Solution to Cater to Users with Limited Technical Skills

Complex technology solutions do not warrant optimal results. As an example, one director in the office of campus life suggested that "*the use of a single hallway phone in each dorm floor instead of room phones seems to be a better solution*". The reason is that this solution increases the chance of at least one student will hear the hallway phone and inform everyone in the hall in the case of an emergency. He added that "*a 40-year old model of communication can be more effective in this case.*" Hence, technology should be a vehicle that facilitates effective human response to incidents so that nobody is left out due to technological complexity or various disabilities. Following this principle, SINERGY shall use simple yet useful solutions that take into consideration the variety of campus constituents including those with disabilities and limited technical skills.

Usability: SINERGY shall use usability and human factors best practices of simplicity to achieve the needs of the stakeholders by adopting popular technologies among students as well as traditional technologies used by faculty, staff, and emergency personnel. In addition, user-facing system interfaces shall make use of simple and efficient design choices to reduce the effect on system performance and scalability especially during emergencies.

5.7. Expected Quality Attributes

Our study focused on the quality attributes that are important to stakeholders. These constitute the attributes that should drive the architecting process. However, as a network-centric system of systems, SINERGY should exhibit a more cohesive set of quality attributes to understand the tradeoffs among them. While implementation of SINERGY will vary based on its operational context, the list below provides key common quality attributes that complement the specific quality attributes presented in the previous section.

Reliability is the extent to which SINERGY provides its capabilities without failure under normal conditions and during emergencies within the specified performance parameters.

Maintainability is the extent to which SINERGY facilitates changes to its components. Four types of maintenance exist [1]. Adaptive maintainability is concerned with adaptations required as SINERGY external environment evolves. Corrective maintainability is concerned with fixing bugs and making corrections to SINERGY components. Perfective maintainability is concerned with enhancements requested because of changing stakeholder requirements. Preventive maintainability is concerned with preventing potential problems for reengineering.

Performance is the extent to which SINERGY executes its tasks in an efficient manner to support the decision-making process of the user.

Scalability is the extent to which SINERGY maintains its functional correctness as its workload is increased within some pre-defined limits.

Survivability is the extent to which SINERGY satisfies and continues to satisfy specified critical requirements (e.g. security, reliability, real-time responsiveness, and accuracy) under adverse conditions.

6. DISCUSSION OF LESSONS LEARNED

The lessons learned from this study go beyond the elicitation of functional and quality needs of SINERGY stakeholders. They provide both practical and theoretical insights into the next generation of GDSS that provide real-time decision support for scenarios requiring context-awareness. In this section, we present these insights in a way that triggers future research questions.

6.1. SINERGY Intended Uses

The main practical contribution of this capabilities specification is intended to provide a framework that guides the architecting, design, and implementation of a real-time context-aware GDSS for campus emergency response management. The list of capabilities provided constitutes a high-level domain analysis from various stakeholder perspectives. Based on this analysis, we classified the intended uses (IUs) for SINERGY capabilities specification into two categories: 1) IUs related to the development of SINERGY architecture specification, and 2) IUs related to the evaluation of SINERGY implementations when operational. This categorization is important because it bounds how these results can be used. Table 6 lists SINERGY intended uses.

Table 6: Intended uses of SINERGY

IUs related to the development of SINERGY architecture specification
Establish interoperability and integration guidelines for SINERGY component systems
Multiple channels of communication between SINERGY stakeholders

Shared understanding of responsibilities related to campus situational awareness, security control, and emergency response management
Support decision makers devise an acquisition strategy of SINERGY capabilities
Contractual reference between decision makers and providers of SINERGY component systems
IUs related to the evaluation of SINERGY implementations when operational
Evaluation of the architecture specification against its required quality attributes
Evaluation of the soundness of architecture decisions and their impact on development
Evaluation of the adherence of SINERGY operational models to established campus emergency, privacy, and legal guidelines
Gap analysis between existing and planned SINERGY capabilities

6.2. Emergency and Decision Making

During emergencies, the outcome of decision-making processes may have a direct impact on life. Any support that can be provided to decision makers to make the most optimal decisions is considered desirable. We conducted interviews to propose a GDSS architecture that can enhance campus safety without diminishing the value of open campus environment. However, key challenges remain to be addressed to ensure continuous improvements to ensure the right information to the right people at the right time for optimized coordination and decision making.

Technology: Typically, organizational structures and business processes influence the way GDSS is designed and used. However, given the ubiquity of the network and the pervasiveness of information-producing and information-consuming devices, the influence should be managed properly to the positive [18]. Information technology has a tremendous influence on organizational structures and business processes now, thereby influencing traditional decision-making processes. Novel approaches to design GDSS for providing a common operating picture and helping decision makers make better decisions and auditing how decisions are converted into action in response to incidents is critical. SINERGY architecture is derived from the interviews that describe the behavior of the users. Given that SINEGY architecture will influence behavior, users' behavior is likely to change requiring new structural changes to SINERGY to address new emerging behaviors. The duality between structure and behavior, and how they influence each other, raises a fundamental question about how decision processes are designed within a useful architecture [2]. More specifically, how to design decision processes into a technology architecture such as a GDSS to facilitate coordinated decision making and assuring safety while preserving an open campus environment with its ever changing student behavior? The ease of updating the GDSS structures and decision making support mechanisms is essential to facilitate accommodating the new behavior on campus. How can the GDSS support distributed decision making using the new technologies that enable us to distribute software over a network providing both autonomy and control to nodes in the network? Next generation GDSS may be viewed as a loosely coupled system of nodes acting as semi-autonomous agents in a coordinated fashion that can learn using a case-based approach. As new technologies become mainstream, their influence on decision-making processes become undeniable warranting their incorporation into new decision-making processes. SINERGY used by campus constituents can influence new decision-making paradigm aiding timely decisions by campus administrators and emergency responders to act and make decisions for the right context.

Augmented Decision Making: Organizations follow established decision-making processes to ensure optimal outcomes. More than any time before, decision-making processes rely heavily on information systems to augment their impact [10]. Augmented decision making is critical, especially during emergencies where information is continuously changing, and may be incomplete, incorrect, or inaccessible. One of the key findings of this study is the importance of distribution of assets to ensure availability and redundant coverage. Availability of assets across various networks allows decision makers to make use of the most current information to form their decisions.

Collaborative Decision Making: Decision making involves consultation with others to ensure consistency of decisions and overall alignment with established processes. In cases of emergencies, collocation of decision makers is not always possible or desirable. Therefore, support for distributed decision making is crucial. Video and audio conferencing technologies provide necessary tools to connect geographically dispersed decision makers to allow collaborative efforts to tackle complex emergency problems and make the best decisions in real-time for the right context.

Case-based Learning: The challenging fact about emergency response is that emergencies evolve from different sets of conditions. It is almost impossible to prepare for a particular instant of an emergency given that there may not be a priori information about how to respond to every incident. Therefore, emergency preparedness focuses on procedures that address types of emergencies rather than instances that may have happened in the past. Case-based learning is a concept that came up in several discussions with stakeholders. It is concerned with the issue of using cases from past incidents to develop self-awareness (i.e., artificial intelligence) in GDSS. Hence, GDSS can help implement case-based reasoning to propose a base solution that may be modified and tailored by human decision makers for new incidents.

When we talk about a system as complex as SINERGY, several challenges surface to the discussion. The study that we conducted allowed us to learn about several issues related to decision-making processes, emergency management, collaboration, and coordination. These lessons, we believe, provide rich topics for further research. We provided a framework for the design of a GDSS for emergency management response for open campus environments and this basic framework should help answer the initial questions in this inquiry.

7. CONCLUSIONS

The capabilities and quality attributes identified herein are intended to provide a framework to guide the architecting, design, and implementation of SINERGY. They are a starting point from which other SINERGY capabilities and quality attributes are identified based on the operational context of a particular implementation of this GDSS.

The outcome of this study shows a clear contrast between what is currently practiced and deployed, and what is actually needed to fully prepare open campuses to man-made disasters. It provides a supporting case to our argument that current technology solutions address the problem from one or few perspectives, when it should be addressed comprehensively. The nature of the problem is multi-faceted and so should be its solution. The next step is to build on these results to develop an architecture that takes into consideration the operational context of a solution implementation. The documentation of such an architecture can be found at this URL: http://manta.cs.vt.edu/sinergy.

Lastly, this study also provides an illustration for the use of capabilities as an alternative approach to determining functionality requirements for guiding the design of complex and useable GDSS. This approach balances between baselining key requirements in the form of capabilities early on in the development life cycle, and the accommodation of requirements volatility inherent in GDSS developments. Therefore, this balanced approach enables GDSS developers to manage system complexity by ensuring that tradeoffs are reasoned about early on before details are addressed as the development moves on to design and implementation.

REFERENCES

[1] Balci, O. and W.F. Ormsby (2008), "Network-Centric Military System Architecture Assessment Methodology," International Journal of System of Systems Engineering 1, 1-2, 271-292.

[2] Bose, I. and X. Chen (2009), "A framework for context sensitive services: A knowledge discovery based approach," *Decision Support Systems 48,* 158-168.

[3] Burstein, F., Brezillon, P., and Zaslavsky, A. (2011), *Supporting real time decision-making: The*

role of context in decision support on the move. Springer, New York, NY. http://dx.doi.org/10.1007/978-1-4419-7406-8.

[4] Campus Technology 2010, "Campus Technology Webcasts /Webinars," Campus Technology, http://campustechnology.com/

[5] DeSanctis, G. and R.B. Gallupe (1987), "A foundation for the study of group decision support systems," *Management Science 33, 5,* 589-609.

[6] DoDAF (2009a), "DoD Architecture Framework Version 2.0 Volume I: Introduction, Overview, and Concepts - Manager's Guide," Architecture Framework Working Group, Washington, DC.

[7] DoDAF (2009b), "DoD Architecture Framework Version 2.0 Volume II: Architectural Data and Models - Architect's Guide," Architecture Framework Working Group, Washington, DC.

[8] DoDAF (2009c), "DoD Architecture Framework Version 2.0 Volume III: DoDAF Meta-model Physical Exchange Specification - Developer's Guide," Architecture Framework Working Group, Washington, DC.

[9] FEMA (2010), "FEMA: What We Do," Federal Emergency Management Agency (FEMA), http://www.fema.gov/about/divisions/mitigation.shtm

[10] Gundersen, D.E., D.L. Davis, and D.F. Davis (1995) "Can DSS Technology Improve Group Decision Performance for End Users? An Experimental Study," *Journal of End User Computing 7, 2,* 3-10.

[11] ICS 2010, "The Incident Command System," Federal Emergency Management Agency (FEMA), http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm

[12] Kim, J.K., R. Sharman, H.R. Rao, and S. Upadhyaya (2007), "Efficiency of critical incident management systems: Instrument development and validation," *Decision Support Systems 44*, 235-250.

[13] March, S. and G.F. Smith (1995), "Design and natural science research on information technology," *Decision Support Systems 15,* 251-266.

[14] Simon, H.A. (1981), *The Sciences of the Artificial (2nd Edition.)*, MIT Press, Cambridge, MA.

[15] Turban, E., J.E. Aaronson, and T.P. Liang (1997), *Decision Support Systems and Intelligent Systems 5th Edition*, Prentice Hall PTR, Upper Saddle River, NJ.

[16] VT (2007), "The We Remember Website," Virginia Tech, http://www.weremember.vt.edu/

[17] VT Review Panel (2007), "The Virginia Tech Review Panel Report – August 2007," The Virginia Tech Review Panel, http://www.vtreviewpanel.org/report/index.html

[18] Zhang, S., and S. Goddard (2007), "A software architecture and framework for Web-based distributed Decision Support Systems," *Decision Support Systems 43,* 1133-1150.