# Engineering resilient information systems for emergency management

C. Vecchiola
H. Anjomshoa
Y. Bernstein
I. Dumitrescu
R. Garnavi
J. von Känel
G. Wightwick

*Resilience is often a qualitative property that is considered fundamental for communities affected by disasters. The concept, along with its variations, has been explored in several domains, such as warfare, business continuity, ecology, computer security, and infrastructure management. The lessons learned constitute a valuable starting point for building resilient socio-technical systems. In previous work, we have described resilience principles at the systems level by reviewing related studies in several research areas. This paper organizes the principles into a conceptual framework for resilient design, which includes a set of nonfunctional requirements for resilience and an assessment methodology for evaluating architectural work from a resilience standpoint. After having presented this conceptual framework, we discuss its application in our collaboration with the Victorian Fire Services Commissioner. This collaboration has led to the specification of a high-level reference architecture for the information interoperability platform that will support emergency services in Victoria.*

## Introduction

*Emergency management* refers to the combination of services, organizations, and people that coordinate to protect lives and assets, and operate before, during, and after the occurrence of disastrous natural or human-made events. Recent disasters in the state of Victoria, Australia, including the Black Saturday bushfires in February 2009, have led the emergency services leadership to revise the concept of emergency management from consisting of single agencies responsible for specific emergencies to a more-encompassing all-hazards, all-agencies approach. Within this new framework, which focuses on the community, the concept of resilience of the socio-technical spectrum has been deemed fundamental for dealing effectively with emergencies. Resilience is a qualitative property of systems that identifies their capability to "cope" with disruptive events and agents, thus minimizing the permanent damage caused to such systems. Although traditionally used to characterize the property of materials to return to their original shape once put under stress, resilience has been applied and used in other contexts (e.g., ecology, psychology, business operations, and computer networks) to express the capability to gracefully degrade under stress, which provides the flexibility for shifting control locally during disruptions and recover as a challenge eases. With reference to emergency management—particularly in Victoria—the concept of *community resilience* or *societal resilience* expresses the capability of the community to withstand disasters and minimize their impact. To achieve this outcome, resilience should encompass the entire life cycle of emergency management from planning and preparation through to emergency response and recovery.

Effective propagation of information plays a crucial role in ensuring emergency-management resilience. Therefore, the technological systems responsible for information management must themselves be resilient so that they can be relied upon during an emergency. Although considerable work has been performed in studying and improving the effectiveness of, and the interactions within, systems of people where technology plays an important role (e.g., socio-technical systems theory [1], cybernetics [2], and management sciences [3]), there have been fewer attempts to isolate the desirable attributes of technology within this context. In particular, there has been limited exploration of resilience as a key property of computing systems and

Digital Object Identifier: 10.1147/JRD.2013.2259432

**0018-8646/13 © 2013 IBM**

the role such systems play in supporting processes and people as a component of the overall socio-technical system. With regard to computing systems, resilience has often been used as a synonym of fault-tolerance and robustness with particular applications of system design, algorithm design, and networking. We believe that there is limited literature addressing resilience in software systems and their architecture in a broader sense. In previous work [4], we have identified general principles that can be used as a starting point to design and implement resilient systems and utilize principles with reference to software systems architecture. In this paper, we provide a more complete conceptual framework that, from the concept of resilience, leads to the definition of resilience requirements for software systems and an assessment method of software architecture from a resilience standpoint. We also discuss an application of this framework in the area of emergency management, by briefly reporting our collaboration with the Victorian Fire Services Commissioner that has led to the definition of a reference architecture for emergency services in Victoria.

The remainder of the paper is organized as follows. In the next section, we provide some background information about the concept of resilience and its characterizing aspects. We then briefly introduce the resilience principles and the conceptual framework in which they exist. We conclude with an overview of the current state of emergency management in Victoria and discuss our work developed in collaboration with the Victorian Fire Services Commissioner.

## Background

As mentioned in the introduction, originally used to denote the property of materials to recover their shape after being put under physical stress, the concept of resilience has been extended to apply to other domains. The term *resilience* is often used in relation to other concepts such as *survivability* [5], *dependability* [6], *resistance* or *robustness*, *vulnerability* [7], and *sustainability* [8].

Research in the military and warfare domains has demonstrated interest in resilience, mostly in terms of survivability. This is the ability of technical systems and operatives to avoid or withstand a human-made hostile environment without suffering an abortive impairment of their ability to accomplish their designated mission [9, 10]. In this context, studies about survivability have primarily focused on improving technologies and techniques for communications. In addition, the concept of variability (in the technologies and protocols used for communication, as well as in the type of communication under different conditions) has been considered important for resilient systems. Moreover, the ability to revert to local control has been considered beneficial for survivability. Reversion to local control means that when links in the command chain are broken, "leaves" possess sufficient autonomy and information about the overall plan to perform effectively until links in the command chain are restored. This can be considered as a form of graceful degradation of the system, because such a technique allows the system to partially function despite that some of its capabilities have been made inoperable. With regard to the specific case of emergency management, the ability to revert to local control has been identified as fundamental to rapidly respond to events [11].

Research in ecology has introduced a new perspective on the topic of resilience. Holling and Meffe [12] were the first to distinguish between *equilibrium resilience* and *ecosystem resilience*. The former denotes the capability of a system to return to an equilibrium-steady state after being subject to perturbations, whereas the latter is essentially characterized by adaptive change, which allows the system to assume a different equilibrium state as a result of perturbations of the previous equilibrium state. Equilibrium resilience fundamentally expresses the original concept of resilience, whereas ecosystem resilience extends it by adding flexibility and adaptation. Holling and Meffe [12] and other researchers [13, 14] have emphasized the importance of the preservation of diversity and variability in ecosystems to foster long-term resilience. With regard to policy-making and the interrelations between society, economy, and environment, the concept of resilience is closely related to the notion of sustainability and sustainable development. In very simple terms, sustainability is the capability of a system to endure. Sustainable development [8] refers to the collection of practices, policies, and technological advancements that makes human development sustainable with regard to its impact on the environment. Therefore, sustainability is a desired property of the processes that take place in resilient systems, so that it is possible to prevent predictable collapses.

Business resilience identifies the combination of operational and technological strategies and services that allow organizations to operate on a day-to-day basis, to exploit opportunities to gain a competitive advantage, and to react promptly to unplanned events [15]. The study of best practices to ensure business resilience has led to the development of standards in several countries such as Great Britain [16, 17] and Australia [18, 19] and by international standards organizations such as ANSI (American National Standards Institute) [20] and ISO (International Organization for Standardization) [21, 22]. Literature reveals that resilience is a process that operates through the entire life cycle of the system. Moreover, it is a dynamic process that needs to be constantly reviewed and adapted to changing conditions.

Research in the area of infrastructure management has focused on the study of robustness and resistance of infrastructure to absorb shocks. Mathematical and physical models have been devised to provide engineers with appropriate tools for building resilient infrastructure. Together with these tools, techniques for implementing graceful degradation are fundamental for implementing resilient infrastructures: load-shedding techniques used to prevent a dam from collapse are an example. Chang and Shinozuka [23], while measuring the resilience of communities from disasters, expressed resilience in terms of redundancy, resourcefulness, robustness, and rapidity. The first two are a means to achieve resilience, whereas the last two are desired ends for resilient systems.

Socio-technical systems, cybernetics, and system sciences that involve the study of the characteristics and the interactions in systems of people from different perspectives have also been used to investigate the concept of resilience. Research in the area of resilience engineering [24] involves the study of systems and methods that enable organizations to become more agile and proactive in assessing risks and make the changes necessary to prevent the failure of systems. Even though mostly focused on providing techniques and tools for safety and productivity management, an important element to ensure system resilience is constant monitoring and assessment of the state of the system, together with the ability to respond proactively to unplanned events.

With regard to applications in software and software systems, resilience has been mostly related to robustness, resistance, and dependability. Researchers and developers in the areas of computer security have identified techniques and methods for making computing systems robust and resistant to attacks, misuses, and corruption [25]. Recovery-Oriented Computing (ROC) [26] and Autonomic Computing [27] represent two initiatives that provide a more holistic approach to computer system resilience. The former focuses on improving the response of a system to faults and on ways to minimize its downtime by providing techniques for system design and implementation allowing a fast recovery (i.e., redundancy, partitioning, fault insertion, diagnosis aid, non-overwriting storage, and orthogonal mechanisms). The latter is a model for designing computing systems that exhibit the autonomic capabilities of the nervous system: self-healing, self-managing, self-monitoring, self-optimizing, self-protecting, and so on. Rather than directly facing the issue of resilience in software, the two research initiatives provide guidance for building software systems that are resilient.

In summary, currently there is no precise definition of the term *resilience* that fully characterizes it in all of its uses. What emerges from our discussion, however, is that there are many elements (e.g., characteristics, properties, and findings) that, when implemented, could lead to more resilient systems. In particular, the concepts of 1) *variability in system processes*, *components, and interactions*, 2) *replication of functions across scales and functional groups*, and 3) *adaptive change* have been mostly drawn from resilience study in ecology. The idea of *graceful degradation* has been primarily inspired by our overview about survivability, resilience in relation to warfare, and infrastructure engineering. Elements such as *robustness*, *resourcefulness*, *rapidity*, and *resistance* are inspired from resilience studies in infrastructure management. The concepts of *big picture* (i.e., a focus on the ends and not the means), *delegation* (in contrast to micro-control), and *flexibility* (in contrast to rigid optimization) mostly derive from socio-technical systems theory and policy management. Characteristics such as *continuous execution monitoring*, *revision*, and *adaptation* (resilience as a continuous process rather than a set of emergency procedures) are based on resilience engineering research. All of these contribute to the formulation of principles for implementing resilience in systems. These are the basis of our conceptual framework.

## A conceptual framework for architectural resilience

The elements previously identified synthesize resilience across different research areas, but they do not provide practical guidance on how to build resilience into systems. In a previous work [4], we have derived a set of principles for system resilience. After having introduced these principles, we discuss a conceptual framework that, by starting from these principles, will introduce a set of tools and concepts that provide practical support for building resilient software systems. These tools and practices can be integrated with existing methodologies for software architecture.

### *Resilience principles*

From the attributes of resilience identified above, it is possible to formulate a set of principles that enucleate the elements of resilience in a set of non-redundant considerations that can be used as a basis for system design. These principles are meant to be general and are not tied to a specific research area.

- **Principle 1.** *Diversity and variability*—Systems that rely strongly on a single approach and/or few components tend to be more prone to single points of failure, which makes them more vulnerable. Multiple variations in methods, procedures, and components help resilience. Such variations are possible in an open context, which favors the implementation of different solutions for the same problem.
- **Principle 2.** *Adaptive change*—Resilience is achieved by a continuous adaptive process that operates across all scales of disruption (from small events to disasters), rather than by introducing ad hoc measures and procedures triggered after the occurrence of the event.

**Table 1** Relation and mapping of the resilience principles to the characterizing elements of resilience as they have been identified in the literature review.

| | *Principle 1* | *Principle 2* | *Principle 3* | *Principle 4* | *Principle 5* | *Principle 6* | *Principle 7* |
|---|---|---|---|---|---|---|---|
| Variability in system processes, components, and interactions | X | | | | | | |
| Replication of functions across scales and functional groups | | | | | | X | |
| Adaptive change | | X | | | | | |
| Graceful degradation to local control | | | | X | X | | |
| Robustness, resourcefulness, rapidity, and resistance | | | | | | X | |
| Big-picture (i.e. determine the ends, not the means) | | | | | X | | |
| Delegation (in contrast to micro-control) | | | | | X | | |
| Flexibility (in contrast to rigid optimization) | | | X | | | | |
| Continuous execution monitoring, revision, and adaptation | | X | | | | | |

- **Principle 3.** *Efficiency trade-off*—An overemphasis on efficiency and optimization is often an obstacle to resilience. Therefore, balance between optimization and flexibility for a disaster event plays an important role.
- **Principle 4.** *Graceful degradation and seamless reintegration*—It is vital for systems and processes to degrade gracefully—by fostering local control, shedding load, and being designed for fail safety—when disruptions occur and reintegrate smoothly (e.g., reinitiate full communication and coordination) as the system recovers.
- **Principle 5.** *Goal-orientation, delegation, and big picture*—The outcomes rather than the means should be highlighted in order to provide a useful perspective during disruption. It is also critical to trade off between self-regulation and central control while having a broader view of a solution and its effects.
- **Principle 6.** *Resourcefulness, robustness, redundancy, and rapidity*—These properties are critical in the face of disruption by providing the capability of finding alternate solutions, strengthening the system components, increasing function accessibility, and leading to a more rapid response. These properties also contribute to make a system secure, which is a fundamental aspect of resilient system.
- **Principle 7.** *Holistic and integral approach*—Resilience is a multidimensional issue encompassing the technical, organizational, social, and economic dimensions.

**Table 1** indicates the relation between these principles and the elements leading to resilient systems identified in the literature reviewed above. With the exception of Principle 7, each of the principles is drawn from one or more elements found relevant in the literature. In some cases, the mapping is straightforward (Principles 1, 3, and 4), whereas in others, the concept expressed by the principle is defined by aggregating similar aspects of these elements. Principle 7 captures the fact that resilience is a qualitative property of systems and that resilience strategies should therefore be holistic and integrated across all aspects of a system.

The principles constitute a set of guidelines and characteristics that are helpful for understanding system resilience from a general perspective. They are a cohesive distillation of the principles discovered in the literature and can be the starting point of a design or an assessment process of a system from a resilience standpoint.

### *Deriving resilience requirements for information systems*

Leveraging the principles described above for building resilient software systems requires an understanding of how they fit into the common practices and methodologies for software architecture and engineering. In particular, there is a gap between the recommendations made by the principles and other artifacts that are more effective and useful for architects and engineers, such as requirements.

Therefore, it is important to explain how to make this transition and how to complement the common practices with the activities for resilience.

There has been considerable research in the area of software architecture and methodologies for building and/or evaluating software architectures. Rozanski and Woods [28] have studied the practice of software architecture design and proposed a general method for defining architecture for software systems based on the concept of *views*, *viewpoints*, and *perspectives*. Sessions [29] provided an overview of the most popular software architecture methodologies for designing and implementing enterprise-scale software systems, and Roy and Graham [30] provided a taxonomy of software architecture evaluation methods. Our goal is not to define a complete and new methodology for software architecture design and evaluation, but to provide architects with a useful guidance and tools to consider resilience effectively while building software systems. Therefore, we will delineate a conceptual framework rather than a methodology. This approach has also been found in some of the most popular enterprise architecture methodologies discussed by Sessions [29], in particular, the use of a matrix-based artifact as a checking tool that can be used throughout the entire process of design. Another key point that emerges from a review of these studies is the importance of engaging all of the relevant stakeholders in the design process. This allows the architect to have a complete view of goals of the system being built.

The process of software architecture starts with identifying the purpose of a software system. This information is obtained by interviewing relevant stakeholders; this helps elicit a complete view of the domain in which the software system operates and to better capture its goals. We can think of the domain as being characterized as a set of dimensions whose combination gives a full representation of it. The interviews with the stakeholders are aimed at identifying these dimensions. By viewing resilience through the lens of each of these dimensions, an expert practitioner will be able to elucidate a general set of requirements for the overall system. To determine these requirements, for each of the domain-specific dimensions, consider what system characteristics are necessary for the resilience principles to apply in this dimension.

The resilience requirements will then be added to the collection of other requirements that give a complete and actionable view to design a software system. This lays the foundation for further processes and methodologies to be employed that will lead to a system design and eventually to its implementation. We believe that the method proposed by Rozanski and Woods [28] is quite useful to adopt, as it allows us to express resilience in terms of an artifact called *perspective*, which is a set of cross-cutting concerns that identify a quality property of a system. This will help us assess whether the design meets its goals or covers the resilience requirement proposed. However, in general, any other method could be applied to design the system.

### Designing and assessing resilient information systems

On their own, resilience requirements do not ensure that resilience is built into software systems; there must also be a process in place to verify that such requirements are implemented. We believe that having a practical and intuitive tool can be more effective than a complex and more detailed process, especially for large-scale systems. Such an intuitive tool could be expressed, for instance, in the form of a matrix, where elements can be easily cross-referenced.

Matrices have been already used as a tool for design or evaluation. For example, Zachman [31] bases a framework for information system architecture on a matrix representation. Rozanski and Woods [28] use a matrix representation to cross-reference the different perspectives of a system with the set of views that define it. For the purposes of evaluating system resilience, we propose a *relevance matrix*, which correlates the resilience principles with architectural aspects that have been deemed by software architects and stakeholders as key for the software systems, and whose combined view gives a general picture of the software system. These aspects are directly connected to architectural choices made for the implementation under assessment. Even though the most appropriate aspects depend on the specific system that is being assessed, we can use a set of general aspects to describe how the matrix works. For instance, we can imagine decomposing a software system into the following components: information flow, data architecture, component distribution, dependencies and relations, process and procedures, and connectivity. These aspects constitute the rows of the relevance matrix, whereas the resilience principles represent the columns (see **Figure 1**). Each of the cells of the matrix will be assigned a *relevance value*, which is a numeric value based on a qualitative scale that gives an understandable but summarized idea of how much a given principle, and a guidance connected to it, is relevant to that specific aspect. By summing the values along the row, we compute an *importance score*, which tells how much the given aspect is globally important from a resilience standpoint. By summing the values along the column, we compute the relevance score, which defines how much a given resilience principle is pertinent to the overall design. We suggest using an integer scale from 1 to 5 to define relevance values, where the smaller values denote lower relevance. In the context of what is being measured, we suggest that a scale of five numbers represents a good compromise between level of detail and simplicity of use.

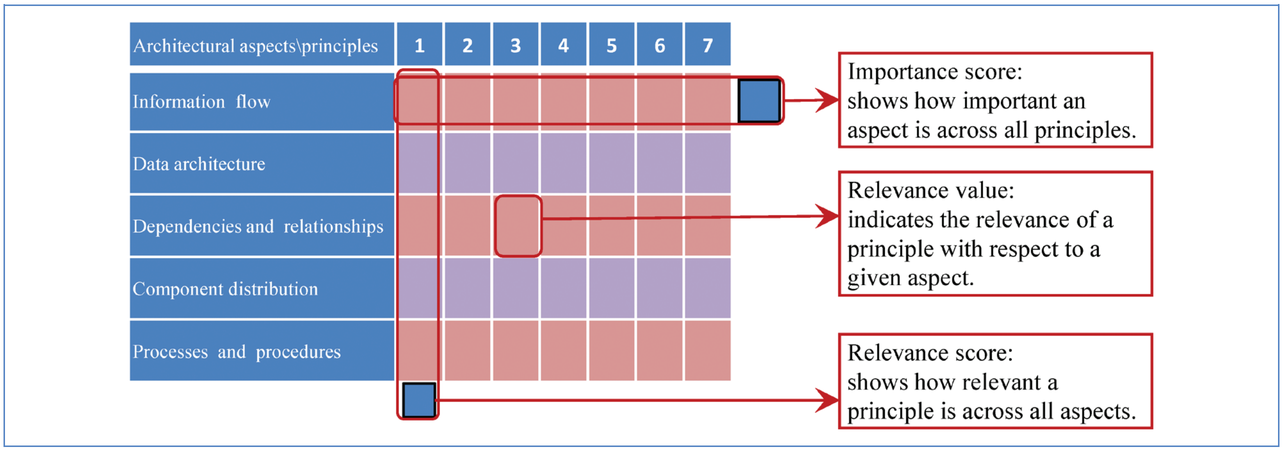
Architectural aspects\principles
1
2
3
4
5
6
7
Information flow
Data architecture
Dependencies and relationships
Component distribution
Processes and procedures
Importance score: shows how important an aspect is across all principles.
Relevance value: indicates the relevance of a principle with respect to a given aspect.
Relevance score: shows how relevant a principle is across all aspects.

Figure 1

A relevance matrix that correlates principles and key architectural aspects.

Once the relevance matrix has been filled with values based on the domain expertise of stakeholders and the experience of software architects and engineers, the relevance matrix constitutes a guidance to verify the implementation of resilience requirements. In practice, the high relevance value of a principle with respect to an aspect suggests that the recommendations deriving from that principle must be implemented in the architectural choices made for the given aspect. By using the reference values, it is then possible to investigate the architectural design through the lenses of resilience and determine whether the choices made are satisfactory. The matrix provides additional guidance: a high relevance score for a given aspect indicates that more than one principle has high relevance for that aspect. This is where two (or more) principles may lead to contrasting architectural decisions when trying to implement all the recommendations. If the principles have different relevance values, it is possible to prioritize the decisions and select among them. In case the relevance values are the same, the importance score of the principle can be of help in selecting which decision to implement.

Moreover, by utilizing the principles and the aspects, the method can also be applied to existing software systems, where the original requirements are no longer accessible or have evolved over time. It is always possible, in fact, to identify the architectural aspects of a system by inspecting it and then build the matrix.

The purpose of the relevance matrix is to provide quick and general guidance in assisting a practitioner in evaluating the resilience of a particular system design. It is not a substitute for the collaborative work of stakeholders and architects and their experience and knowledge in the respective fields.

## Resilient software systems for emergency management

### *Emergency management in Victoria*

The most common types of large-scale emergency events in the state of Victoria are floods and bushfires. While both have a substantial economic impact, bushfires are responsible for the most loss of life. On February 7, 2009, in Victoria (a date that is now referred to as Black Saturday), a sequence of record hot days with high winds preceded by almost two months of little or no rain led to fast-spreading intense bushfires that killed 173 people and destroyed thousands of homes. As a consequence of this disaster, the Victorian Bushfires Royal Commission (VBRC) [32] was established to examine events surrounding the Black Saturday fires and to answer questions raised about the emergency response.

In the case of fire in Victoria, three agencies are principally involved in managing emergency services. They are the Metropolitan Fire Brigade (MFB, responsible for responding to fires within metropolitan Melbourne), the Country Fire Authority (CFA, responsible for fire response in rural and regional Victoria, as well as the outer suburbs of Melbourne), and the Department of Sustainability and Environment (DSE, responsible for fire management on public land, accounting for approximately one third of the surface area of the state). The VBRC identified inadequate integration between these agencies as one of the reasons why operations performed by the emergency services were not as efficient as they could have been. Moreover, according to the commission, the lack of access to up-to-date and relevant information about unfolding events was one of the major reasons for the impaired response of the community as a whole to these events.

The findings of the VBRC also led to the establishment of the new role of Fire Services Commissioner, whose primary responsibility is to oversee and work with the three fire services of Victoria, "leading, enabling, and facilitating changes to the way fire services work together with partners and the community to *prepare* for major fires and *operate as one*" [33]. We emphasize here that the community and the partners of the three fire services (e.g., Victorian Government, Victoria Police, Emergency Services Telecommunications Authority, Bureau of Meteorology, and VicRoads) have been identified as stakeholders, and their role in the management of catastrophic events has been recognized. It is worth noticing that the resulting set of stakeholders spans a variety of organizations driven by their own business goals, and that the Fire Services Commissioner has only direct influence on the three emergency-management agencies cited previously. The acknowledgment of this fact constitutes an important step forward in conceiving the role of emergency management in the community.

The Fire Services Commissioner has identified the need for an improved information architecture for the emergency services, one that values input from all stakeholders and enables a common operating view that is always accessible to everyone. This view should be accessible to those formally involved in emergency management and even those that, through circumstances, become part at any level of emergency-management operations and need to make decisions. It is the belief of the Fire Services Commissioner that the quality of the decisions made depends on the information available at the time of decision-making, and that having correct, reliable, and timely information at all times is crucial. To realize this vision and make information efficiently available to all stakeholders who need it, new information technology and tools need to be integrated in the way agencies operate and communicate.

Technological advances in recent decades have led to significant increases in computational power, the growth of the Internet, and an explosion in the quantity and accessibility of information. In addition, mobile and interconnected devices have become commonplace. However, emergency services have not fully exploited these changes. This has had an impact on their engagement with the community, their response to emergency situations, and the level of interagency cooperation. The current infrastructure deployed for emergency services is typically built on a foundation of separate ("siloed") agency-specific systems and is based on voice communications. Although voice-based communications have been at the center of emergency services for more than 50 years, analog voice information is largely inaccessible to computers. This results in inefficient routing of information, often performed by people not systems. As a consequence, significant delays in making crucial data widely available are frequently observed. According to the VBRC [32], "An effective flow of information is crucial to the Incident Management Team's ability to formulate a strategy for managing community protection, fire response, and firefighter safety."

The community is particularly disadvantaged by the current information infrastructure. Once an emergency takes place, the situational awareness of the community is often limited to official warnings along with potentially inaccurate information from traditional and social media. Likewise, community contributions to situational awareness rarely extend beyond the placement of 000 (equivalent to 911 in the United States) emergency calls. Thus, the community is largely excluded from either contributing to or benefiting from a common operating picture. This has been seen as a particularly critical flaw to address.

### *The information interoperability blueprint and VINE*

In collaboration with the Victorian Fire Services Commissioner, we have contributed to the development of a framework and technology solution for the information interoperability challenges affecting emergency management in Victoria, as described in the previous section. Such a system must satisfy a number of requirements, and key among these is the embodiment of system-wide resilience characteristics in order to support critical emergency-management tasks. The nature of our collaboration required us to focus on designing a resilient information system for information sharing in an emergency-management context. Although such a system is critical to the resilience of the overall socio-technical emergency-management apparatus, this discussion does not address the process for achieving resilience for emergency management in general.

An important step in helping key stakeholders to gain an understanding of the nature and importance of resilience principles was to discuss these principles with experts well versed in the operational issues associated with emergency management. As discussed while introducing the conceptual model, in order to devise a truly resilient architecture, it is necessary to understand and consider the dimensions in the target domain—both technical and organizational—along which resilience is required. In the case of emergency management, we identified five dimensions that were particularly crucial for the system. These dimensions are represented diagrammatically in **Figure 2** and are discussed next.

*Organizational structure* is certainly one of the elements that affect emergency-management operations. These structures are the result of the collective effort of a variety of stakeholders, often belonging to different chains of command. As illustrated in Figure 2, there are a variety of organizational structures that exhibit different characteristics with regard to the effectiveness of action and the related flexibility in facing diverse situations.

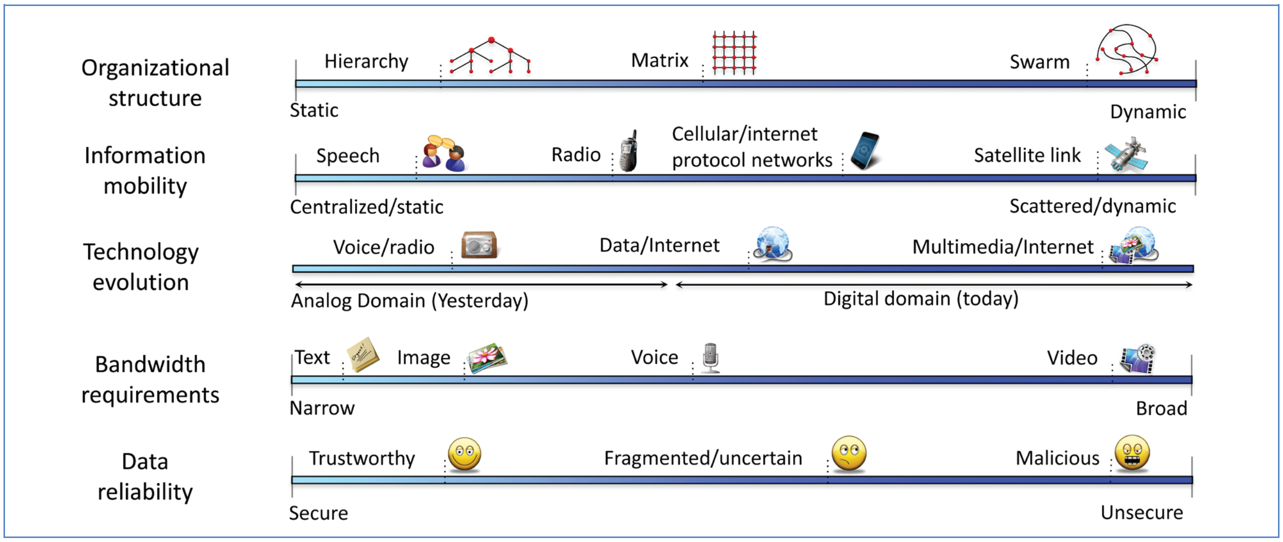

Figure 2

The dimensions of the problem domain across which resilience is investigated.

Hierarchical organizations are very effective in terms of chain of command but are somewhat rigid, whereas swarm structures are extremely flexible but less effective in terms of global coordination and control. Our collaboration with the emergency-management agencies has revealed that even though there is a reference hierarchical structure during large-scale events, emergency-management arrangements often require being more dynamic. This dimension also covers the way in which the data is maintained, transmitted, and shared among the relevant stakeholders. For instance, in a hierarchical structure, the command chain can also be used to transmit data, whereas in peer-to-peer and swarm structures, broadcasting can be more appropriate.

The *mobility of information* is another dimension of interest. This not only refers to the technological solutions that allow the information to be delivered where needed, but also includes the procedures and conventions that have been adopted over time by either emergency services or the community to acquire and dispatch information. There has been a transition from a situation in which most of the information was based on in-person communication into an environment where the source of relevant information for an incident is the whole community, which uses a variety of methods and techniques to communicate.

*Technology evolution* is definitely an important aspect to consider: in the last 50 years, digital technologies have supplanted analog technologies in a broad range of domains. Although this generally has improved system capabilities, there is still value in considering analog solutions, especially in the case of emergency management. For instance, disruptions or catastrophic events might prevent use of digital solutions. Furthermore, some stakeholders (e.g., elderly people) may not have effective access or make effective use of digital technologies. This leads us to consider another aspect, which we considered sufficiently important to be treated as a separate dimension: *bandwidth requirements*.

Different technologies have different requirements in terms of bandwidth, and this affects not only their accessibility and coverage but also the amount of information that can be conveyed. It is important for the effectiveness of emergency-management operations to select the appropriate amount of information to communicate and the most appropriate medium, rather than using one technology versus another.

*Data reliability* is another dimension that becomes important, especially when we consider that, over time, a core aspect of traditional and reliable data, such as official warnings, has been increasingly supplemented by a larger volume of less reliable data, such as media reports and social media information. These new sources of information cannot be ignored, as they may improve information coverage and freshness, but they must be carefully and appropriately interpreted.

The domain-specific dimensions formulated above can be used by an expert practitioner alongside the broader principles defined earlier as a guide for the distillation of a set of requirements for such a system. Our research on resilience and interviews with some key emergency-management stakeholders have provided evidence that resilience can be better achieved through a comprehensive approach rather than a "best compromise" solution. In other words, the set of requirements we derive should emphasize the importance of coping with all the relevant variations across these dimensions, rather than selecting only a specific solution. For instance, the information system should support and make use of rich multimedia data feeds, but if users lose their high-bandwidth wireless connection, the system should be able to make a transition to transmitting less bandwidth-intensive forms of data across a slower connection.

The IBM Research team combined the conceptual framework with its own software architecture expertise, as well as the knowledge gained through numerous interviews and discussions with domain experts in the area of emergency management, to specify a suitable set of requirements, as follows:

- **Requirement 1.** *Stakeholder ecosystem*—The system must address the needs of a heterogeneous set of community stakeholders and provide appropriate ways to interact and collaborate.
- **Requirement 2.** *Informed decision-making*—The system must be able to support informed decision-making at all levels and in any conditions.
- **Requirement 3.** *Security, robustness and diversity*—The system must be capable of delivering information despite disruptions, with different levels of service and by making use of different strategies and channels. It must also be secure against attacks that deny service at critical times, that provide unauthorized access to the system, or that attempt to contaminate the system with misleading or inaccurate information. Moreover, it must have in place redundant procedures to implement a given functionality, especially for core and critical features.
- **Requirement 4.** *Coherent high-level system architecture*—The system should be designed such that any disruption—from a minor perturbation to a large-scale disaster—is addressed consistently. Conceptually, the same system and set of procedures should be used to address any type of event.
- **Requirement 5.** *Graceful degradation and seamless reintegration*—The system must be capable of gracefully degrading its behavior and performance when disruptions occur. In the same way, disconnected systems should be able to operate independently and reintegrate seamlessly as the impact of disruptions ceases.
- **Requirement 6.** *Information integration*—The system must integrate and make use of diverse information and information channels. These should include sensory data, social networks, weather observations, forecasts, geospatial information, etc.

These requirements have been validated by domain experts in emergency management and embodied in the Information Interoperability Blueprint (“the Blueprint”), which constituted the next phase of our collaboration with the Fire Services Commissioner. This is a document for a wide audience that establishes the vision for a future information system for emergency management in Victoria, known as the Victorian Information Network for Emergencies (VINE). VINE is envisaged as a web services-based integration platform for all information about an emergency from many different sources, giving controlled access to that information to all stakeholders in an emergency. As an integration platform, VINE will make it possible to assimilate a broad variety of information currently stored in different formats across a variety of siloes. The platform will also have a powerful API (application programming interface) that provides flexible programmatic access to this information. This latter capability serves as a foundation for the emergence of an ecosystem of tools that improve community resilience and the effectiveness of the emergency response capability of Victoria. Furthermore, the Blueprint specifies that a variety of advanced data analytics and decision-support tools will be developed using the platform, providing access to such tools to a broader set of stakeholders.

The Blueprint potentially addresses the entire Victorian community. Therefore, the language and concepts used to express the requirements are less formal and more accessible to a wider audience. In particular, it envisions the emergency management in an information-centric world as being: engaged with the community, resilient, open, mobile and multimedia capable, holistic, and a platform for innovation. Furthermore, it specifies the necessity for the system to be diverse, redundant, adaptable, capable of graceful degradation and seamless reintegration, and comprehensive. This group of properties covers in total the requirements expressed above. The Blueprint has been reviewed by operational and management leaders within the emergency services and formally endorsed at the government level. This demonstrates a successful contribution of our research effort and approach to the definition of a new vision for emergency management in Victoria.

The current phase of our collaboration with the Fire Services Commissioner involves the creation of a high-level reference architecture based on the principles and goals for VINE as described in the Blueprint. The reference architecture will guide further architectural work for incrementally implementing the vision of VINE. This work will provide the opportunity to use the remaining key component of our conceptual framework: the relevance matrix. We hope to report on our experience with this process in a future publication.

## Final considerations

In this paper, we have described our research on system resilience and introduced a conceptual framework for designing resilient information systems. We reported our experience in applying the concepts of this framework in the domain of emergency management in the course of our collaboration with the Victorian Fire Services Commissioner.

Our work on the characterization of resilience for systems has been organized into a group of concepts and artifacts that can support the work of architects and software engineers in embodying resilience in the design of systems and verifying it is properly implemented. The key elements of this framework are the resilience principles, resilience requirements, and the relevance matrix. The principles identify general assumptions about system resilience, from which resilience requirements for a specific system are derived. This is done by understanding the application domain of the systems and perspective of each the involved stakeholders. The relevance matrix constitutes a quick assessment tool and guidance for architects and engineers while performing architectural work or assessing an existing system. By not defining a methodology but rather a conceptual framework, these elements can be easily integrated with the existing approaches and architecture methodologies.

The collaboration with the Victoria Fire Services Commissioner, which originally motivated our work on resilience, represented an opportunity to apply the framework in real life. We can observe that the concepts developed in the framework have been definitely useful, even though their use has often been implicit rather than methodical. In particular, we noted that the application of the guiding principles to a specific application domain has required considerable work, mostly because of the diverse points of view of the complex network of emergency-management stakeholders in Victoria. A key role, in ensuring the acceptance of the resilience requirements expressed, has involved the Information Interoperability Blueprint, which is a non-technical document that expresses a vision for a resilient information system underpinning emergency management in Victoria. This document has established a path for a more formal characterization of the VINE. In addition, at present, we only made use a subset of the conceptual framework introduced in this paper. In the future, we expect to complete the evaluation of our conceptual framework by applying the relevance matrix to proposed architectural designs of VINE. The results obtained so far are promising, as the Blueprint has been reviewed by operational and management leaders within the emergency services and formally endorsed at the government level.

## References

1. K. B. DeGreene, *Sociotechnical Systems: Factors in Analysis, Design, and Management*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1973.
2. N. Wiener, *Cybernetics, or Communication and Control in the Animal and the Machine*. Cambridge, MA, USA: MIT Press, 1948.
3. K. Boulding, "General systems theory—The skeleton of science," *Manage. Sci.*, vol. 2, no. 3, pp. 197–208, Apr. 1956.
4. J. von Känel and C. Vecchiola, "Global technology trends: Perspectives from IBM Research - Australia on resilient systems," *Int. J. Comput. Sci. Eng.*, vol. 8, no. 3, 2013.
5. R. Ellison, D. Fisher, R. Linger, H. Lipson, and N. R. Mead, "Survivable Network Systems: An Emerging Discipline," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-97-TR-013, 1997.
6. A. Avižienis, J. C. Laprie, and B. Randell, "Fundamental Concepts of Dependability," LAAS-CNRS, Toulouse, France, Res. Rep. 1145, 2001.
7. W. N. Adger, , M. Janssen and E. Ostrom, Eds."Vulnerability," *Global Environ. Change*, vol. 16, *Special Issue on Resilience, Vulnerability and Adaptation*, no. 3, pp. 268–281, Aug. 2006.
8. United Nations General Assembly. (1987). Our Common Future: Report of the World Commission on Environment and Development, Geneva, Switzerland, Transmitted to the General Assembly as an Annex to document A/42/427—"Development and international cooperation: Environment; Our common future, Chapter 2: Towards sustainable development". [Online]. Available: http://www.un-documents.net/ocf-02.htm
9. *Aerospace Systems Survivability Handbook Series: Volume 1. Handbook Overview*, JTCG/AS-01-D-002, Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), Arlington, VA, USA, 2001.
10. *Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automation Information Systems (MISAS) Acquisition Programs*, , Regulation 5000.2-R, App. 3, Department of Defense, US Government, Washington, DC, USA, 2002.
11. *Australian Emergency Management Arrangements*, Attorney-General's Department, Commonwealth of Australia, Barton, Australia, 2009. [Online]. Available: http://www.em.gov.au/Documents/Australian%20Emergency%20Management%20Arrangements.pdf
12. C. S. Holling and G. K. Meffe, "Command and control and the pathology of natural resources management," *Conserv. Biol.*, vol. 10, no. 2, pp. 328–337, Apr. 1996.
13. S. S. Light, L. H. Gunderson, and C. S. Holling, *The Everglades: Evolution of Management in a Turbulent Ecosystem, Barriers and Bridges to the Renewal of Ecosystems and Institutions*, L. H. Gunderson, C. S. Holling, and S. S. Light, Eds. New York, NY, USA: Columbia Univ. Press, 1995, pp. 103–168.
14. G. D. Petersen, C. R. Allen, and C. S. Holling, "Ecologycal resilience, biodiversity, and scale," *Ecosystems*, vol. 1, no. 1, pp. 6–18, Jan. 1998.
15. G. M. Otteson, "How resilient is your business?," *Packet, Cisco Syst.*, vol. 17, no. 1, pp. 30–34, 1st Quarter, 2005.
16. *Business Continuity Management. Code of Practice*, British Std. Inst. (BSI), BS 25999-1:2006, 2006. [Online]. Available: http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030157563
17. *Business Continuity Management. Specification*, British Std. Inst. (BSI), BS 25999-2:2007, 2007. [Online]. Available: http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030169700
18. G. Love and C. Gibson, *A Practitioners Guide to Business Continuity Management*, Standards Australia, HB 292-2006, 180 p., 2006. [Online]. Available: http://www.qsp.org.br/pdf/HB292-2006.pdf
19. *Executive Guide to Business Continuity Management, Australia*, Std. Australia, HB 293-2006, 2006. [Online]. Available: http://infostore.saiglobal.com/store/Details.aspx?ProductID=568884
20. *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements With Guidance for Use*, ANSI, ANSI/ASIS SPC.1-2009, 2009ASIS Int., New York, NY,

*Trademark, service mark, or registered trademark of International Business Machines Corporation in the United States, other countries, or both.

**Trademark, service mark, or registered trademark of Google, Inc., or The Open Group in the United States, other countries, or both.

USA. [Online]. Available: http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

21. *Societal Security—Preparedness and Continuity Management Systems—Requirements*, TC 223. ISO/CD 22301, 2011. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038
22. *Societal Security—Business Continuity Management Systems*, TC 223. ISO/CD 22313, 2012. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50050
23. S. E. Chang and M. Shinozuka, "Measuring improvement in the disaster resilience of communities," *Earthquake Spectra*, vol. 20, no. 3, pp. 739–755, Aug. 2004.
24. E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. Hampshire, U.K.: Ashgate Publ. Co., 2006.
25. K. S. Trivedi, D. S. Kim, and R. Ghosh, "Resilience in computer systems and networks," in *Proc. ICCAD*, New York, NY, USA, 2009, pp. 74–77.
26. D. Patterson, A. Brown, P. Broadwell, G. Candea, M. Chen, J. Cutler, P. Enriquez, A. Fox, E. Kiciman, M. Merzbacher, D. Oppenheimer, N. Sastry, W. Tezlaff, J. Traupman, and N. Treuhaft, "Recovery-Oriented Computing (ROC): Motivation, Definition, Technologies, and Case Studies," Dept. of Comput. Sci., Univ. of California, Santa Barbara, CA, USA, Tech. Rep. CSD-02-1175, 2002.
27. J. O. Kephart and D. M. Chess, "Vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003.
28. N. Rozanski and E. Woods, *System Architecture Working with Stakeholders Using Viewpoints and Perspectives*. Reading, MA, USA: Addison-Wesley, 2005.
29. R. Sessions, "A Comparison of the Top Four Enterprise Architecture Methodologies," ObjectWatch, Inc., Houston, TX, USA, MSDN Online. [Online]. Available: http://msdn.microsoft.com/en-us/library/bb466232.aspx
30. B. Roy and T. C. N. Graham, "Methods for Evaluating Software Architecture: A Survey," School of Comput., Queen's Univ. at Kingston, Kingston, ON, Canada, Tech. Rep. 2008-545, 2008.
31. J. A. Zachman, "A framework for information system architecture," *IBM Syst. J.*, vol. 26, no. 3, pp. 276–292, 1987.
32. *2009 Victorian Bushfires Royal Commission Final Report*. [Online]. Available: http://www.royalcommission.vic.gov.au/commission-reports/final-report
33. *Building New Foundations*, Fire Services Commissioner, Victoria, Australia, , 2011. [Online]. Available: http://www.firecommissioner.vic.gov.au/wp-content/uploads/Building_new_foundations_Fire_Services_Commissioner_VIC1.pdf

*Received November 16, 2012; accepted for publication December 18, 2012*

**Christian Vecchiola** *IBM Research - Australia, Carlton, VIC 3053, Australia (christian.vecchiola@au.ibm.com).* Dr. Vecchiola is a Research Scientist at the IBM Research - Australia laboratory. He currently leads the "Systems of Systems" Research Initiative that investigates models and technologies for flexible decision-making in complex and heterogeneous domains. He joined IBM Research - Australia in June 2011 and since then has led the research on resilience and its application to technologies and systems of people in the area of disaster management. Prior to joining IBM, he worked at the University of Melbourne as a post-doctoral fellow and lead software engineer in the Cloud Computing and Distributed Systems Laboratory with a major focus on research and development in the area of cloud computing middleware. He holds a Ph.D. degree in computer engineering and has conducted his doctoral studies on engineering complex and dynamic distributed systems with agent technologies.

**Hamideh Anjomshoa** *IBM Research - Australia, Carlton, VIC 3053, Australia (hamideh.a@au.ibm.com).* Dr. Anjomshoa joined IBM Research - Australia in October 2011. She obtained her Ph.D. degree in mathematics from the University of South Australia. Her research interests include various aspects of optimization for industries. She has authored several research papers in mining optimization published in high-ranked journals.

**Yaniv Bernstein** *IBM Research - Australia, Carlton, VIC 3053, Australia (ybernst@au.ibm.com).* Dr. Bernstein is a Researcher and Software Engineer at IBM Research - Australia. He has a Bachelor of Computer Science degree from the University of Melbourne and a Ph.D. degree in the area of document management and information retrieval from RMIT University. His interests include information retrieval, data warehousing, high-dimensional approximate search, cloud computing, and the interaction between research and development in building successful software systems. Prior to joining IBM in early 2012, Dr. Bernstein spent five years at the Google engineering office in Zürich, Switzerland, where he led a number of projects across Google Search**, Google Maps**, and YouTube**. Dr. Bernstein is currently working in the disaster-management area as part of Smarter Planet Initiative of IBM Research.

**Irina Dumitrescu** *IBM Research - Australia, Carlton, VIC 3053, Australia (irina.dumitrescu@au.ibm.com).* Dr. Dumitrescu obtained her Ph.D. degree in operations research from the University of Melbourne (Australia) in 2002. She has been working on optimization problems arising in diverse sectors including transportation, logistics, defense, natural resources, and energy. She has worked with universities and research centers from Romania, Australia, and Canada, and held a Marie Curie Research Fellowship in Germany. Prior to joining IBM Research - Australia in 2011, she worked with the University of Melbourne pursuing her recent interest in geothermal energy. Her scientific work in the area of operations research has been published in top journals and in books and has been awarded several prizes.

**Rahil Garnavi** *IBM Research - Australia, Carlton, VIC 3053, Australia (rahilgar@au.ibm.com).* Dr. Garnavi received her Bachelor's degree in software engineering from Amirkabir University of Technology (Tehran, Iran) in 2003, and her Master's degree in artificial intelligence from Isfahan University (Isfahan, Iran) in 2005. She completed her Ph.D. degree in 2011 at the University of Melbourne, Department of Electrical and Electronic Engineering, developing a computer-aided diagnostic system for skin cancer (melanoma). She joined IBM in June 2011. While her main engagement is in healthcare, she has interest and involvement in disaster management and software architecture. She also holds an honorary research fellowship position in the Department of Computing and Information Systems at The University of Melbourne. Dr. Garnavi has authored numerous research papers in medical image analytics, presented at conferences and published in peer-reviewed journals. Some of her work experience in industry includes business analysis and data modeling, and software design, development, and testing.

**Jürg von Känel** *IBM Research - Australia, Carlton, VIC 3053, Australia (jvk@au.ibm.com).* Dr. von Känel is the Senior Manager of the IBM Research - Australia lab in Melbourne. He studied math and computer science at ETH (Eidgenössische Technische Hochschule) Zürich and holds a Ph.D. degree in computer science (1991). He joined IBM in 1985 in Zürich, Switzerland. In 1991, he moved to the IBM Thomas J. Watson Research Center in the United States where he managed the relationship between Research and the financial services industries. In 2004, he initiated an Enterprise Risk and Compliance Framework focused primarily on the financial industry. This led to the *Treasury & Risk* magazine listing him as one of the 100 most influential people in finance in 2006. Since June 2011, he has moved to Melbourne, Australia, to lead the establishment of the new IBM Research lab in Australia. He is a member of the IBM Academy of Technology.

**Glenn Wightwick** *IBM Research - Australia, Carlton, VIC 3053, Australia (glenn_wightwick@au.ibm.com).* Mr. Wightwick is an IBM Distinguished Engineer, the Director of IBM Research - Australia, and the IBM Australia Chief Technologist. From 2001 to 2006, he undertook a number of assignments in Shanghai, Tucson, and New York in areas ranging from large-scale system design to managing a team defining the architecture of IBM enterprise storage subsystems. Since joining IBM in 1987, he has worked on the application of large-scale UNIX** systems to the solution of complex problems in domains that included computational chemistry, seismic processing, weather forecasting, transaction processing, and highly available infrastructures. He spent seven months working on IBM RS/6000* systems to support the XVIII Olympic Winter Games in Nagano, Japan, during 1997 and 1998, and was involved in the design, implementation, and operation of the RS/6000 infrastructure to support the Sydney 2000 Olympic Games. He has led numerous systems and software development projects, has published a number of papers in the areas of numerical weather prediction, medical imaging, and the Internet, and he holds 12 patents. He is a Senior Member of the Institute of Electrical and Electronics Engineers, was elected to the IBM Academy of Technology in 2000, has served a three-year term on the Australian Research Council College of Experts, and in 2011, was appointed to the Information Technology Industry Innovation Council of the Australian Government. He is an Honorary Professor at the University of Melbourne and was elected Fellow of the Australian Academy of Technological Sciences and Engineering in 2012.