SCIFED Publishers

Bahman Zohuri, SF J Artificial Intel, 2018, 1:3

SciFed Journal of Artificial Intelligence

Review Article Open Access

A General Approach to Business Resilience System (BRS)

*[1]Bahman Zohuri, [2]Masoud Moghaddam

*[1]University of New Mexico, Electrical Engineering and Computer Science Department, Albuquerque, Galaxy Advanced Engineering (CEO), New Mexico USA
[2]Masoud Moghaddam, Galaxy Advance Engineering Consultant, Albuquerque, New Mexico USA

Abstract

Artificial intelligence (AI) is one of those technologies that seems to be expanding its reach in every direction. This technology will take center stage at Think 2018. The J Resilience thinking is inevitably systems thinking, at least as much as sustainable development is. In fact, "when considering systems of humans and nature (social-ecological systems) it is important to consider the system as a whole." The term "resilience" originated in the 1970s in the field of ecology from the research of C.S. Holling, who defined resilience as "a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables." In short, resilience is best defined as "the ability of a system to absorb disturbances and still retain its basic function and structure."

Introduction

In the earliest of Egyptian times, men saw and knew about the power of beasts, and seem to have envied them. There is a sense that humans, at the dawn of civilization, were subject to, and seemingly inferior to, the world's more feral inhabitants. However, as man's intellect grew, together with his ability to control, or at least defend himself from wild beasts, so too did his confidence. Many scholars believe that mixed images such as the Sphinx symbolize humankind's domination over wild beasts, and over chaos itself. Such images as the Great Sphinx may very well represent animal power tamed by human intelligence and thus transformed into divine calm. Traditionally, mixed, or composite images were, always seen as divine. One way or another, what could be more dangerous and powerful, or more self-assured than the king of the jungle with the mind of a human king.

In today's world of cyber war, where power of internet allows the variety of cyber-attack have power to prevent them ahead of the time even by seconds is an advantage to the enterprises. Other threats and countering them with properly requires different kind of Sphinx that defend the enterprises and organization against these threats whether is manmade or a natural disaster. We must protect ourselves in fast pace ever changing computer world by taking the advantages of vast world of structured or unstructured data, or other means such as information coming out from geopolitical or human intelligence perspective, to be able to make write choice of action or interaction to our advantages.

Early Egyptian where symbolizing these Sphinx with symbolization of human head on body of a lion, as it is evident from remaining of Great Sphinx Today as it is illustrated here in figure 1. The human head and eyes in it was presentation of Vigilant Eye of the Sphinx to protect and guard a king and his/her kingdom against any adverse

*Corresponding author: Bahman Zohuri, University of New Mexico, Electrical Engineering and Computer Science Department, Albuquerque, Galaxy Advanced Engineering (CEO), New Mexico USA. E-mail: bahmanz@aol.com

Received July 29, 2018; Accepted September 04, 2018; Published September 15, 2018

Citation: Bahman Zohuri (2018) A General Approach to Business Resilience System (BRS). SF J Artificial Intel 1:3.

events that might have a threat to their kingdom. Such evidence can be, found in ancient Babylon and Persian kingdom in the form of standing lion with human head known as Ishtar and its eight gates to inner city.

Figure 1: Remaining of Great Sphinx in Egypt

The Ishtar Gate was the eighth gate of the city of Babylon (in present-day Iraq) and was the main entrance into the great city. It was a remarkable sight; the gate was, covered in Lapis lazuli glazed bricks, which would have rendered the façade with a jewel-like shine. Alternating rows of bas-relief lions, dragons, and aurochs representing powerful deities formed the processional way. The message of course, was that Babylon was protected, and defended by the gods, and one would be wise not to challenge it. The magnificent gate, which was dedicated to the Babylonian goddess Ishtar, was once included among the Seven Wonders of the Ancient World until it was replaced by the Lighthouse of Alexandria in the 3rd century BC. Today, a reconstruction of the Ishtar Gate, using original bricks, is located at the Pergamon Museum in Berlin.

Considering the fact, that Babylon civilization goes beyond any other ancient kingdom; they were the pioneer in the symbolization of Ishtar.

For us in modern world computation and handling of information in the form of cloud system, existence of an autonomous and intelligence system in place is a necessity, and we like to call it a Business Resilience System (BRS), which is the foundation of this text write up.

1.1 Resilience and Stability

Stability and sustainability in any point of life cycle of a system in place or a process within a system is very critical and important for performance and driving efficiency of that system or process from day-to-day operations. Therefore, having a resilience and stability idea within system or process to carry capacity is closely, related to the idea of sustainability. Here we are going to explore another closely related idea of resilience. Resilience is a property of all systems and is related to how a system responds to a disturbance or stressor. In rough terms, the more resilient a system is, the larger a disturbance it can handle [1].

To understand resilience with more precision, we need to first, understand the concept of system state. A system's state is the general configuration that system is currently in it. For example, if we think of a glass jar as being a system, then smashing the jar into little pieces would be a change to the system's state. On the other hand, as an example, if we think of a farm as being a system, then neglecting the farm for so long that it grows into a forest would be a change to the system's state.

What qualifies as a state change depends on how we define the system. There are often many ways of defining a system, so there will also be many ways of defining its states and changes to them. We should have the mental flexibility to imagine systems and states being, defined in different ways, so that we can define them in a more helpful way for our purposes.

Given this understanding of system state, we can now define resilience with more precision.

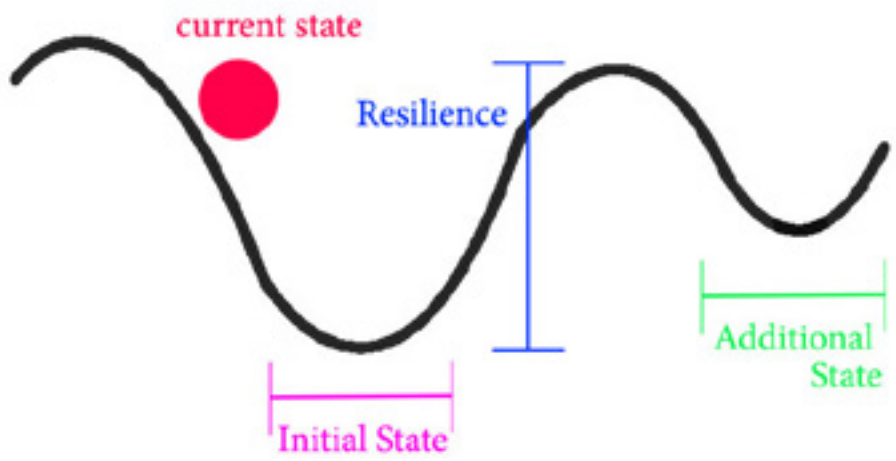
- Resilience is the ability of a system to maintain certain functions, processes, or reactions after experiencing a disturbance.

Let us continue with the jar metaphor, and imagine that the jar is a system for holding sand. The system components would then be the glass jar, the lid, and the sand and air inside the jar. If our glass jar system is, thrown at a wall with enough force, it will smash into little pieces and will no longer be able to perform its principal function

of holding sand, or anything, for that matter. However, what if the force of impact, was only strong enough to crack the jar without breaking it apart? In this case, one of the system components the jar is changed, but the system can continue to hold sand, and thus the system state remains essentially the same. The jar system's resilience, then, is the size of the impact it can withstand without smashing to pieces. Remember that disturbances always change systems in some way (otherwise, we would not call them disturbances). The more a system is able to maintain its functions and components after a disturbance, the greater its resilience to that disturbance.

With simple systems like the glass jar filled with sand, resilience can be (and often is) represented using the metaphor of a ball in a basin. If the ball is pushed a little bit, it will return to the bottom of the basin, i.e., to its initial state. If the ball is pushed hard enough it will leave the basin and eventually settle somewhere else, i.e., in an additional state. The height of the basin thus corresponds with resilience: the higher the basin, the harder of a push the ball can withstand and still return to its initial state. Of course, this metaphor becomes less helpful with more complex, systems, where we are having many constituents, processes, and functions in effect at the same time. In reality, most systems are only relatively resilient to most disturbances. Most complex systems are able to maintain some, but not all, constituents, processes, and functions after any given disturbance (as long as it is not catastrophic). In other words, resilience in real-world systems is usually relative to the type of disturbance and specific constituents, processes, and functions. Figure 2 is illustration of resilience and state for metaphor of a ball in a basin.

Figure 2: Resilience and State (Courtesy of Yooinn Hong)



Resilience is often, viewed as a good thing. If an ecosystem is resilient, or if human society is resilient, then they will be quite capable of withstanding the disturbances that they face. For any system to sustain any particular state, the system cannot experience any disturbances that exceed its resilience for that state. Thus resilience, like carrying capacity, and is closely, related to sustainability. This is why we see efforts to enhance resilience from groups like the Resilience Alliance [2]. They would like our human-environment systems to be sustained.

However, whether, or not resilience actually is good is an ethical question, and the answer is not automatically yes. We will discuss ethics further in Module 3, but for now, consider this. A terrorist network might be resilient if it can withstand many attacks or other efforts to destroy or disrupt it. Likewise, a dangerous pathogenic virus might be resilient if it can withstand many antiviral medicines or other measures that we take to curtail the virus. In these two cases, resilience is not a good thing. At least, we can imagine that in these cases, some people might reasonably consider resilience to be, bad. Therefore, while resilience is certainly an important concept and may often be, considered as a good thing, we should not blindly assume that it always is.

As far as the stability of resilience system is concerned, one important concept related to resilience is its stability. Stability is the opposite side of the disturbances a system faces. If there are few disturbances or small disturbances, then the system is relatively stable. If there are many disturbances or large disturbances, then the

system is relatively unstable.

Stability is a very important concept in agriculture as an example. We would very much like it if our farms would yield (produce) about the same amount of food each year, because in general we eat about the same amount of food each year. If there is an unusually large food yield one year, this can cause complications but is typically not a huge problem.

However, if there is an unusually small food yield in one year, then this can be a larger problem and it may cause a huge shortage in products and increase in prices or even chaos. In the agriculture module, we will examine yield stability in more detail. There, we'll discuss the Irish Potato Famine, which occurred in the mid-1800s. This was a case of extreme instability in food yield, which had disastrous consequences.

One might think that a resilient system would be one with more stability, but this is not always the case. Sometimes, some instability or disturbance can help to increase resilience. This occurs when the disturbances increase the system's ability to respond to further disturbances.

For example, think of our bodies as systems. If we do not exercise regularly, then we gradually lose our ability to withstand against disturbances which have negative effect on our bodies like joint and muscle weakness which leads to further instability and finally collapsing. Then such instability sends our body to a different weaker state. On the contrary, as we get more exercise, then there is an increase in disturbance and instability in our body in a positive way which increases our ability to withstand further exercise without collapsing and therefore more stability of our body at the end. In this example; the exercise is a positive disturbance, and instability and as we exercise more, our bodies get less stability but more resilience. This often happens with other systems, too [2].

Resilience and intelligent systems along with their engineering is becoming a new paradigm for complex systems performance and maintenance, decision making for survivability of organization and enterprise, Business Process Management (BPM) and Business Continuity Management (BCM).

The concept of resilience was introduced by Holling (DS Holling) [3] in the field of ecology and has been well-documented in ecological and social literature and in some management cases. The initial definition of resilience is that it determines the persistence of relationships within systems and is a measure of the ability of these systems to absorb changes of state in variables, driving variable and parameters to the desired state and yet to be able to function accordingly and still persist.

Also, other definitions can be described and included like:

✓ The potential of particular configuration of a system to maintain its structure and functionality in the face of any disturbance

✓ Or, to have the ability in the system to reorganize following disturbance-driven change and measured by size of stability domain", and "the capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity and feedback.

An intelligent and autonomous resilience system built on data infrastructure should be able to handle its functional fidelity and to be able to take a proper counter-measure facing unpredictable or predictable events, no matter if it is manmade or a natural disaster. For resilient system to have such fiduciary responsibility and to be persistent there is a demand of real-time accessibility to trusted data coming from various directions based on cloud computation and real-time analysis based on fuzzy logic. However, more research has been, done on the concept of resilience and its applicability to ecological, social, and business systems in comparison to engineered systems.

Resilience engineering or Resilience Business System in case of main subject of this book represents a major step forward by proposing a completely new vocabulary instead of adding one more concept to an existing lexicon. Although various definitions of resilience exist that are dependent on the subject area, resilience in infrastructure system, such as, energy system or financial system (banking) has a different concept.

Such systems driven by trusted data in real-time are able, to take proper measures, to adapt and recover from external shocks, including natural, artificial and technological disasters and failures.

On the other side, poor infrastructure and design ultimately affects the smooth and efficient operation of systems and may have a serious interruption in existence of enterprise BPM and BCM accordingly. However, such affect in day-to-day operations of the system, demands a shift of processes, tactics, strategies, coordination and measurement utilizing tools such as cloud computation to collect the right-information from right and trusted data.

This information may come in to dash-port

monitoring screen in the infrastructure systems by triggering the decision-making points that are set per Service Level Agreement (SLA) in place.

Infrastructure systems in most cases are interconnected via Enterprise Service Bus (ESB) or Cloud System (CS). Therefore, analysis of the system should consider interdependency properties, because of both dependencies and interdependencies connectivity and interoperability. Due to these circumstances, there are various types of effects and few can be named here as follows:

1. Cascading Effect: When disruption in one infrastructure; causes disruption in a second,

2. Escalating Effect: When disruption in one infrastructure exacerbates an independent disruption of a second infrastructure; and last but not least,

3. Common Cause Effect: When a disruption of two or more infrastructures occurs at the same time.

The last is more prevalent during natural disasters. The interactions create a very delicate spider web effect between infrastructures as well as feedbacks and complex topologies at different levels.

Therefore, it is nearly impossible to analyze the behavior of any infrastructure in isolation of its environment and surroundings [3].

Therefore, it is nearly impossible to analyze the behavior of any infrastructure in isolation of its environment and surroundings [3].

The basic elements of all the infrastructures are vulnerable to physical and natural disruptions and techno genic disasters. The many interrelationships among the infrastructures call for analysis in which various system components are interrelated and for management strategies that allows easy adjustment as more information and data becomes available. Many different characteristics are, shared among the interdependent infrastructure systems, including but not limited to the following:

1. They are large-scale dynamics, nonlinear, spatially distributed "system of systems" with various components,

2. They are administered by different organization/ agencies with different objectives,

3. They have multiple decision makers/stakeholders (i.e., man in the loop) and sometime conflicting and competing objectives.

Considering the general characteristics of these infrastructures, including their inherent complexity, each has a unique field of research. The traits of "system of systems" will include systems that follow different deterioration patterns, hence they fall under different monitoring and maintenance policies and governing rules, defined by different SLA base on stakeholders.

A critical concept and model of infrastructure dependencies has to address both the level and the interconnectedness. In most cases, some of the analysis and the methods are coincided at various levels. One notable characteristic of the hierarchy is that at the top level, socioeconomic, gaming, scenario techniques are used, and at the lower level more experimental and technical simulation are used.

For instance, if we consider a Business Continuity Plan (BCP), which is a plan to help ensuring that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a natural event such as earth quake, fire or manmade catastrophes such as terrorist acts or any other similar case, where business is not able to function under normal conditions. Thus, having a reliable and intelligent Business Resilience System (BRS) in place could be the most proactive protection of shareholder value against the adverse impact of business disruption at any scale and is the next step beyond BCP.

These very effective risk management approaches can be, shown as follows and supported by the illustration in Figure 3 as business resilience lifecycle.

Steps involved in effective risk management are:

- Enables an organization to become resilient to small and large disruptions

- Defines an early warning approach to identifying and dealing with disruptions versus having to recover from potentially disastrous events

- Drives systematic identification and management of critical business processes, assets and risks

- Provides systematic monitoring and alerting of risk to critical business processes and assets

• Allows for proactive, automated and informed responses to mitigate the impact from disruptions

• Emphasizes mission resource dependencies equally – not just technology

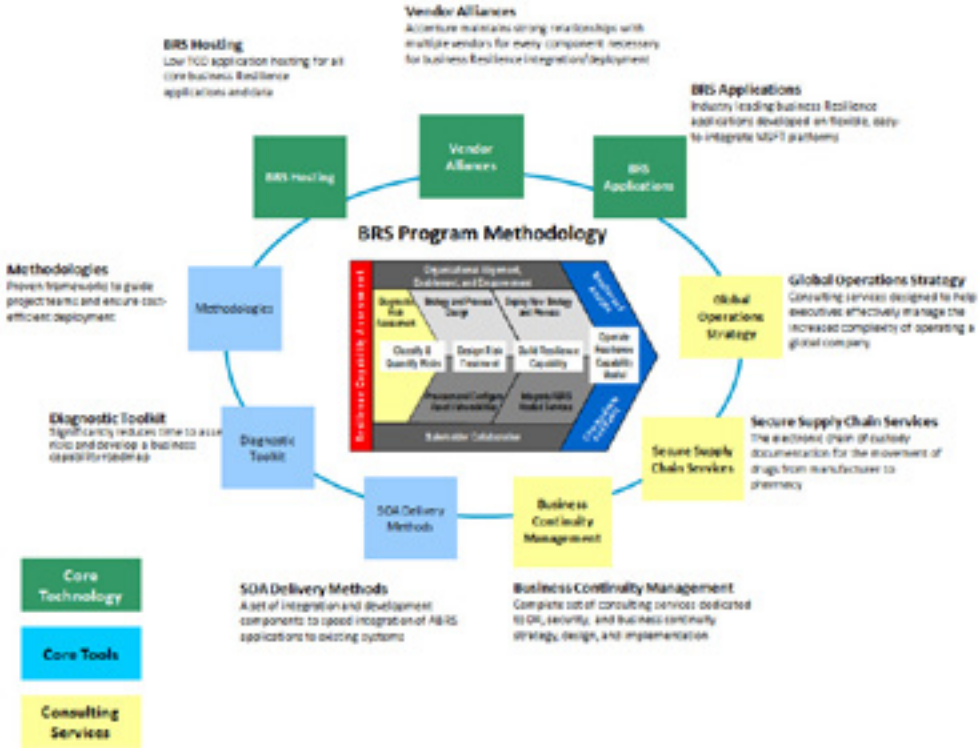
The fundamental challenge now is to develop resilience indices and workflow that can be used within the "system of systems" framework and use cases, given the complexity and some properties of interdependencies of different infrastructures. Such indices built in an autonomous resilience system should be capable of analyzing the resiliency of the overall system.

Furthermore, inclusion of uncertainties that require the opinion of experts can substantially increase the complexity of a particular decision, location, and form of disruption in many situations. Although, we commonly listen to and deal with experts, and in most cases these subject matter experts are knowledgeable in the field but may have limited information by not having enough trusted data. Therefore, imperfect information can still be, used to come up with the optimal decisions for Disaster Recovery (DR) as an example.

In summary, we can show an optimal Business Resilience System (BRS) overview, components offered by figure 4 here.

Figure 3: Business Resilience Lifecycle

Figure 4: BRS Offering Overview Components



It is notable to state that there are several topical areas related to control resilience of a system. These complement the fundamental concept of dependable or reliable computing by characterizing resilience in regard, to the particular control system concerns, including design considerations that provide a level of understanding and assurance in the safe and secure operation of enterprise or organization. These areas are, presented below with discussion to characterize the basis for consideration as an area of resilience.

A. Human Systems

The human ability to quickly understand novel situations by employing heuristics and analogy can provide additional control to system's resilience. On the other hand, there are situations in which we may have a general inability to reproducibly, predict human behavior. This may be true in situations of fatigue or high stress or decision making under high levels of uncertainty. Bayesian methods provide one method by which to take into, account evidence regarding human response, but this is one among many approaches. The literature in human reliability analysis provides an orientation regarding ergonomics, workload, complexities, training, experience, etc., which may be used to characterize and quantify human actions and decisions.

Digital technology, used to benefit control system interaction, can come from the operator's perspective and provide additional complexity. For example, more information can be presented to the human operator to form a response. However, the response could be completely automated and act as an autonomous, human manipulated, or a combination of both. The dependencies and rules for these complex interactions, or mixed initiative, are not necessarily well defined or clear.

Resiliency results from understanding of this complexity by adding human factor and designing an error tolerant control system, which complements perception, fusion, and decision making.

B. Complex Cloud Network

As control systems become more decentralized, the ability to characterize interactions, performance and security becomes more critical to ensuring resilience. While more decentralization can provide additional reliability due to implicit redundancy and diversity, it may also provide more avenues or vectors to cyber-attack. Therefore, the design of complex networks needs to consider all factors that influence resilience, and optimize the flow of information for multiple considerations [4].

Global stability is often, perceived as something that can be achieved by local minimization of all process unit operations, many of which are contained in a facility. However, there is no assurance that global stability can be, achieved in this manner, and in addition, this philosophy maintains a reactionary control paradigm by its nature.

However, considering the latencies in digital control systems, there is a tendency as well as a desire to provide faster responses when the feedback and response occur close to the point of interaction with the application. Therefore, it is, suggested that a true global optimization coupled with a local interaction can achieve both the assurance of a global minima, and an acceptable response when designing control system architecture.

A. Cyber Awareness

Because of the human element of a malicious actor, traditional method of achieving reliability cannot be, used or implemented to characterize cyber awareness and resilience. Dynamic mechanisms of probabilistic risk analysis that can link human reliability with the system state are still maturing. The intellectual level and background of the adversary makes stochastic methods unusable due to the variability of both the objective and the motives.

In addition, the strength of the adversary is increased because the existing control system architecture is not random, and response characteristics are reproducible. Therefore, a resilient design can find strength in similar fashion by becoming a typical normal control system architectural design, and appearing random in response and characteristics to the adversary.

The above discussion provides a holistic and conceptual framework and brief overview of the architectural considerations of control system as part of sub-component and component of a smart business resilience system and more details will be provided in the following chapters and sections of this book.

1.3 Reactive to Proactive Safety through Resilience

In a world of finite resources, irreducible uncertainty and multiple conflicting goals, safety is, created through proactive resilient processes rather than through reactive barriers and defenses. Building a solid infrastructure based on different facets of resilience as the ability of systems to anticipate and adapt to the potential for surprise and failure, or unpredictable events, whether

manmade or natural disaster is a fundamental requirement for today's organizations and enterprises. These fundamental requirements guarantee the survivability of organizations and enterprises from Business Process Management (BPM) and Business Continuity Management (BCM) perspective.

Until recently, the dominant safety paradigm was based on searching for ways in which limited or erratic human performance could degrade a well-designed and 'safe system'. Techniques from many areas such as reliability engineering and management theory were used to develop 'demonstrably safe' systems. The assumption seemed to be; once that safety is established, it can be maintained by requiring that human performance stay within prescribed boundaries or norms. Since 'safe' systems needed to include mechanisms that are guarded against people as unreliable components, understanding of how human performance which could stray outside these boundaries could become important.

According to this paradigm, 'error' was something that could be categorized and counted. This led to numerous proposals for taxonomies, estimation procedures and ways to provide the much-needed data either structured or unstructured, for error tabulation and extrapolation. Studies of human limits became important to guide the creation of remedial or prosthetic systems that would make up for the deficiencies of people.

Since humans (as unreliable and limited as system components) were assumed to degrade what would otherwise be flawless system performance, this paradigm often prescribed automation as means to safeguard the system from the people in it. In other words, in the 'error counting' paradigm, work on safety is comprised of protecting the system from unreliable, erratic, and limited human components or more clearly (protecting the people at the blunt end in their roles as managers, regulators and consumers of systems from unreliable 'other' people at the sharp end who operate and maintain those systems) [5].

Efforts to improve the safety of systems have often (some might say always) been dominated by hindsight, both in research and in practice which perhaps is more surprising in the former than in the latter.

The practical concern for safety is usually, driven by events that have happened, either in one's own company or in the industry as such. There is a natural motivation to prevent such events from happening again. In concrete cases they may incur severe losses of equipment and/or of a life in general cases because they may lead to new demands for safety from regulatory bodies, such as national and international administrations, organizations, business enterprises, and agencies. New demands are invariably, seen as translating into increased costs for companies and are for that reason alone undesirable.

However, this is not, an inevitable consequence, especially if the enterprise takes a longer time perspective. Indeed, for some businesses it makes sense to invest proactively in safety, although such cases are uncommon. The reason for this is that sacrificing decisions usually are considered over a short time horizon in terms of months rather than years or in terms of years rather than decades.

Finding the best optimum and intelligent BRS, requires fundamental research and engineering design for software and hardware to interact with each other in a rather real-time circumstance, where cloud computation based on data is involved.

In the case of research, i.e., activities that take place at academic institutions rather than in industries and are, driven by intellectual rather than economic motives, the effects of hindsight ought to be less marked. Research by its very nature should be looking to problems that go beyond the immediate practical needs, and hence address issues that are of a more, principal nature.

When researchers in the early 1980s began to re-examine human error, and collect data on how complex systems had failed, it soon became apparent that people actually provided a positive contribution to safety through their ability to adapt to changes, gaps in system design, and unplanned situations.

Many studies of how complex systems succeeded and sometimes failed found that the formal descriptions of work embodied in policies, regulations, procedures, and automation were as incomplete as models of expertise and success. Analysis of the gap between formal work prescriptions and actual work practices revealed how people in their various roles throughout systems always struggled to anticipate paths toward failure, to create and sustain failure-sensitive strategies, and to maintain margins in the face of pressures to increase efficiency.

Overall, analysis of such circumstances taught us that failures represented breakdowns in adaptations directed at coping with complexity while success was usually obtained as people learned and adapted to create safety in a world fraught with hazards, trade-offs, and multiple goals [5, 6].

In summary, these studies, revealed [4]:

• How workers and organizations continually revise their approach to work in an effort to remain sensitive to the possibility for failure.

• How distant observers of work, and the workers themselves, are only partially aware of the current potential for failure.

• How 'improvements' and changes create new paths to failure and new demands on workers, despite or because of new capabilities.

• How the strategies for coping with these potential paths can be either strong and resilient or weak and mistaken.

• How missing the side effects of change is the most common form of failure for organizations and individuals.

• How a culture of safety depends on remaining dynamically engaged in new assessments and avoiding stale, narrow, or static representations of the changing paths (revising or reframing the understanding of paths toward failure over time).

• How overconfident people have already anticipated the types and mechanisms of failure, and the strategies they have devised are effective and will remain so.

• How continual effort after success in a world of changing pressures and hazards is fundamental to creating safety.

In the final analysis, safety is not a commodity that can be, tabulated. It is rather, a chronic value 'under our feet', which infuses all aspects of practice. Safety is, in the words of Karl Weick [7], a dynamic non-event. Progress on safety therefore ultimately depends on providing workers and managers with information about changing vulnerabilities and the ability to develop new means for meeting these.

The initial steps in developing a practice of business resilience system have focused on methods and tools:

• To analyze, measure and monitor the resilience of organizations in their operating environment

• To improve an organization's resilience vis-à-vis the environment

• To model and predict the short- and long-term effects of change and line management decisions on resilience and therefore on risk

This book charts an effort by these authors to layout a practical and intelligent Business Resilience System Driven through Boolean, Fuzzy Logics and Cloud Computation.

1.4 The Business Resilience System Backdrop

Backdrop for BRS can be summarized as follows:

Organizations have significant capability in Risk Management and BCP, but the focus is on a narrow subset of high-level risk and they often fail to actively address operational risks that may result in degradation rather than "destruction" of operational capabilities.

A "BRS" seeks to extend organizations' Risk Management and BCP efforts to address threats to the processes that support their primary operational capabilities the primary source/driver of business (shareholder) value.

• Research has shown that even the result of degraded operations has significant impact on shareholder value.

• Organizations generally monitor operational capabilities using KPIs which are lagging indicators.

• BRS identifies and monitors leading indicators of potential impacts to resources that support critical business processes and drive shareholder value.

• BRS is a holistic, enterprise approach to proactively protect shareholder value against the adverse impact of business disruption at any scale, thereby allowing organizations to become more resilient to service degradation without having to invoke BCP steps because of unplanned, destructive events.

• Becoming more resilient allows an organization to rapidly recover from a disruption and resume normal operations with limited revenue, cost and time impacts.

The importance of business resilience cannot be overstated, and it can be depicted as Figure 5 in case of let say stock market analysis, when a supply chain malfunction is announced, stock prices plunge on average and shareholder wealth decreases by certain amount per company.

Current business continuity plans are fragmented and do not include a holistic approach to identifying and

Figure 5: Illustration of BRS Importance

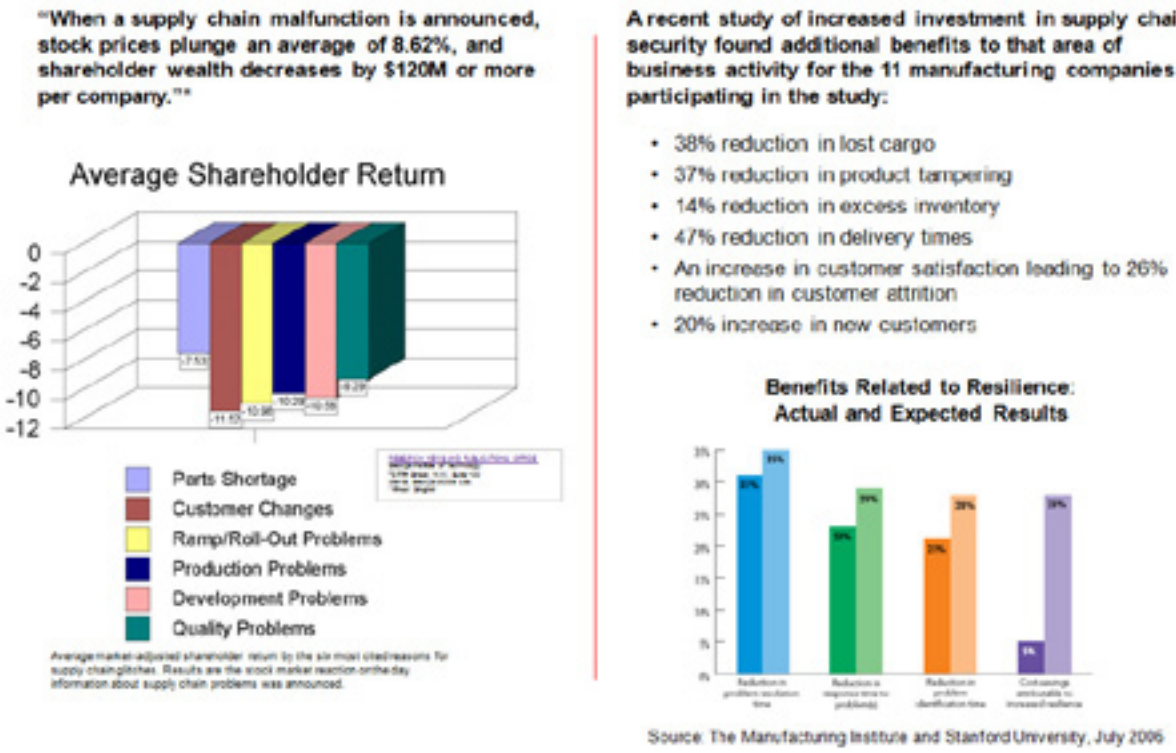
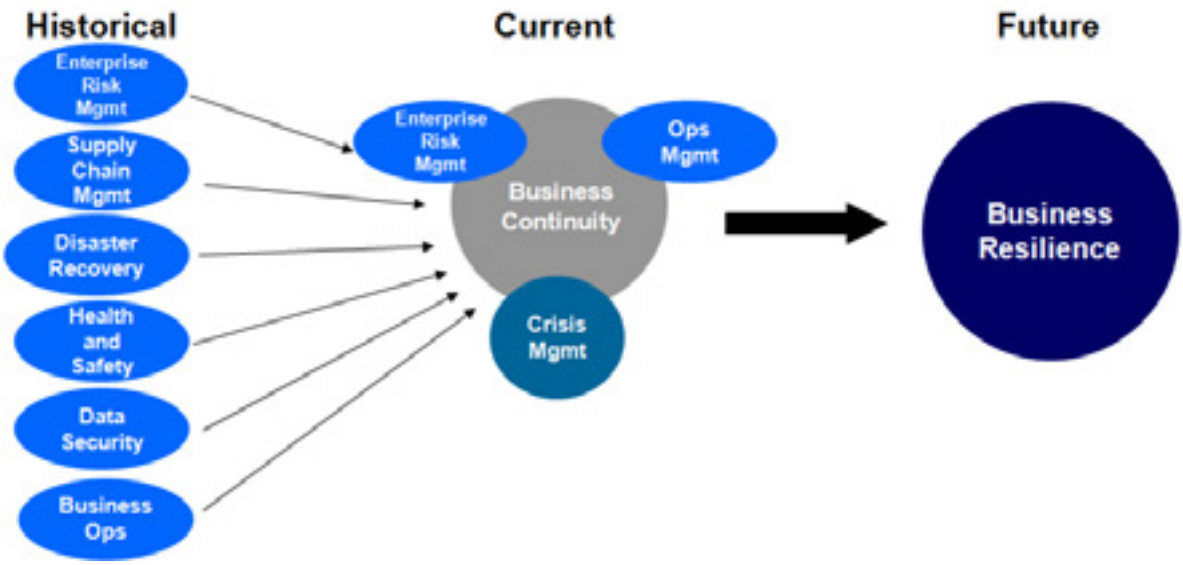


Figure 6: Business Resilience System Historical Path



effectively managing risk to the enterprise. This statement can be seen in Figure 6, that illustrates the key characteristic of historical path, current and future elements of business resilience to a futuristic and intelligent form.

We can also present this historical path in the following form as Figure 7, as a summary to be:

In today's world of cyber threat and cyber-attack, we are in desperate need of a smart business resilience system to be in place. Thus, we can suggest a holistic BRS that has capability of reducing the magnitude and duration of a business disruption as Figure 1-8., presented in following illustration.

Such BRS infrastructure will be responsive to today's threat of cyber-attack, a need for homeland security, business continuity of enterprise from BCM, BPM and BCP, point of view.

Figure 7: Key Characteristic of BRS

	"Incomplete"	"Fragmented"	"Centralized"
Key Characteristics	▪ Silos ▪ Extended response time ▪ Limited reporting ▪ Inconsistent access to information ▪ Minimal collaboration capabilities ▪ Narrow subset of risks ▪ Insufficient risk awareness ▪ Incomplete and non-integrated performance measures	▪ Overlapping components ▪ Moderate response time ▪ Extended reporting capabilities ▪ Some integrated access to information ▪ Moderate collaboration capabilities ▪ Moderate risk awareness ▪ Focused on KPIs which are lagging indicators of performance ▪ Reacts only after an disastrous event occurs	▪ Unified presentation of data ▪ Instant response time ▪ Robust reporting capabilities ▪ Fully integrated access to information ▪ Inherent collaborative capabilities ▪ On-demand risk status and readiness assessments ▪ Utilizes BPIs which are leading indicators of performance ▪ Proactively manages small disruptions to be prevent a disaster

Figure 8: Illustration of Business Impact versus Time

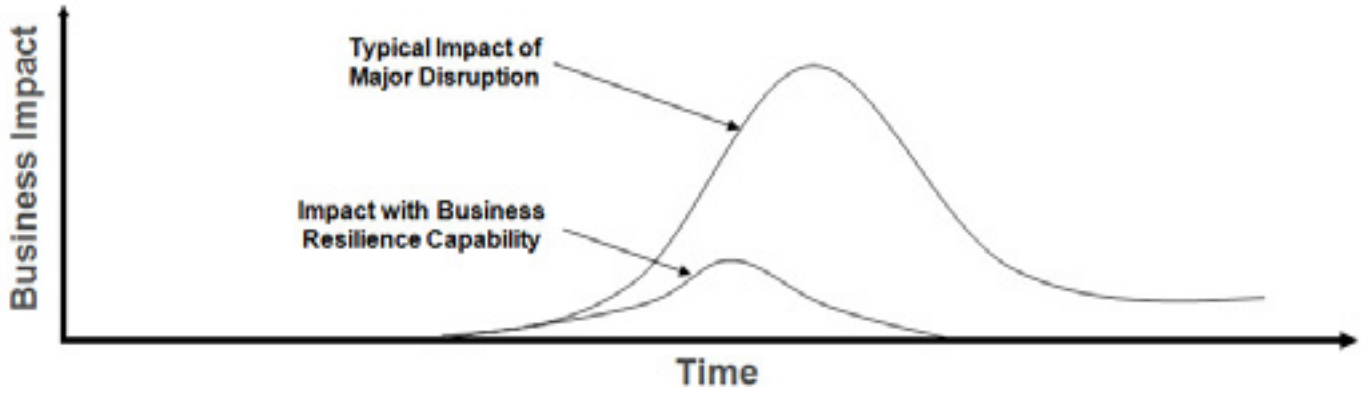


Figure 9: Tabulation of Typical Impact and Resilient Impact

	Latent Risk	Threat Exposes Vulnerability	Disruption Identified	Business Responds	Business Recovers	Business Adapts
Typical Impact	Risks are not clearly assessed, quantified and categorized	Limited ability to monitor threats and vulnerabilities on a real time basis	Reactive notification and awareness of disruptions	Slow and uncoordinated response	Inefficient recovery model leads to excessive costs	Limited processes for assessing performance and improvement
Resilient Impact	Risks are continuously evaluated and managed centrally	24/7 monitoring and alerting capability provides early warning	Early detection arms the right people with the information they need to act	Pre-determined collaboration and action plans are put in motion	Business recovers rapidly as planned	Performance metrics are reviewed and used to make improvements

The granular step-by-step of plot depiction of Figure 8 could breakdown to Figure 9, where we can see tabulation of Typical Impact and Resilient Impact.

As we stated before, the suggested Business Resilience System (BRS), is the proactive protection of shareholder value against the adverse impact of business

disruption at any scale and is the next step beyond BCP, in support of BCM and BPM. This was holistically, presented in Figure 3 and then it was, expanded to Figure 4 sort of showing the offering overview of BRS components.

The secret sauces to the suggested BRS approach by these authors, involves the identification and utilization of the, what we call it is the "*Risk Atom*". The risk atom is comprised of various inter-related and continually moving and interacting components that are arranged in orbits surrounding a process data point (a PDP – the nucleus) and helps a business organization maintain resilient processes through an effective resource response to direct and indirect threats manifested by some preceding event.

This approach helps an organization to:

✓ Better identify, quantify and respond to risks at the business process level

✓ Define the Risk Atoms that are appropriate to a specific business process (a business process may contain one or multiple Risk Atoms)

✓ Identify and quantify those events and threats that could "force" the movement of a Risk Atom across identified and calculated performance measure thresholds over time

✓ Identify and quantify resource responses to avoid, mitigate, transfer or recover from the impact of a threat on a Risk Atom

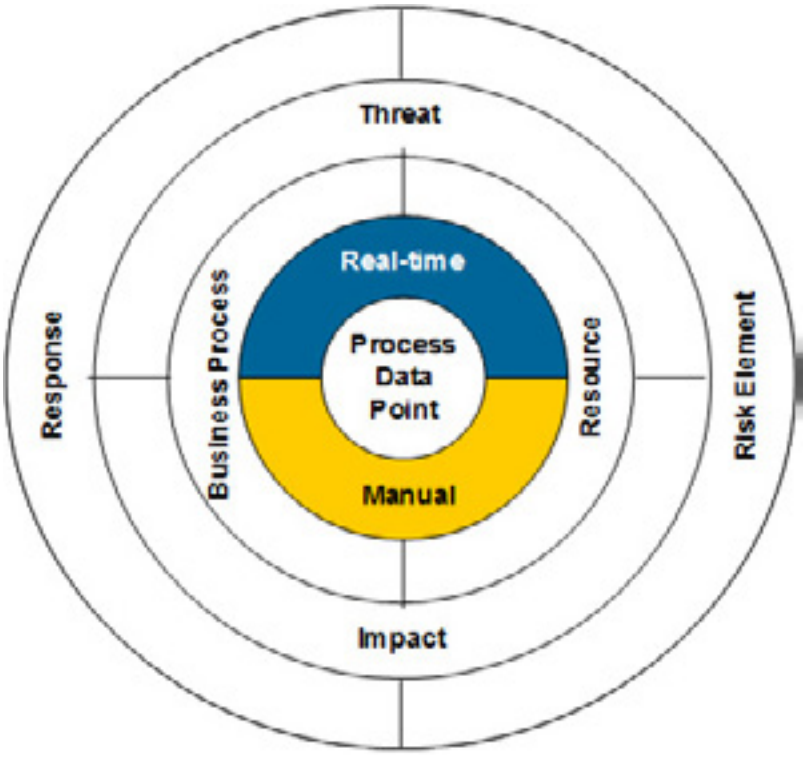
✓ Quantify the level of threat impact that would "force" the Risk Atom to traverse through various performance level thresholds

✓ Determine how to identify and quantify the overall level of risk to a Risk Atom, business process and enterprise

✓ Set the stage for the establishment of an "early warning" approach that would enable an organization to respond to threats and their impact before a catastrophic situation materialized.

The Risk Atom concept can be applied to all business processes and is applicable to just about any "system" that must be resilient and to have a solid BCM and BPM in place. The Risk Atom is the foundation upon which the BRS solution is built and determines the business actions to be taken upon threat manifestation. This solution is illustrated in Figure 10 as follows where data processing through cloud computation as nucleus of this risk atom is either Fuzzy Logic or Boolean Logic or combination of both.

Figure 10: The BRS Risk Atom



The BRS Risk Atom is composed of those inter-related business intelligence "particles" that help a business define the Processing Data Points (PDPs) to be monitored, the impact upon the business and critical business processes as those PDPs pass through various threshold levels, and the business' response to a situation where the PDP is affected.

The Risk Atom is comprised of four (4) orbits of company-specific intelligence which is needed to effectively manage a Critical Business Process CBP) as follows:

- **First Orbit:** Processing Data Point (PDP – the nucleus), with Real-time or Manual reporting capabilities
- **Second Orbit:** Business Processes and accompanying Resources
- **Third Orbit:** Threats to the PDP and Impacts to the business and process
- **Fourth Orbit:** Business Risk Elements and Responses to the threats acting upon the PDP.

For any critical business process there may be one or multiple Risk Atoms, but any Risk Atom must reflect a critical business process measure that, when "tipped", it will begin degrading process capabilities and if left unchecked, it will result in a disaster/destruction situation requiring the invocation of a Business Continuity Process (BCP).

A PDP can move through various levels of thresholds (as, a result of threat manifestation) which will determine the type of business activities to be performed to remedy any foreseeable process degradation before it becomes process destruction.

To fully, understand the Risk Atom and its function within BRS, component parts must be, identified and defined. These component parts are depicted in Figure 11 and they are explained to some details.

Figure 11: Overview of Risk Atom Orbits

The PDP (Process Data Point)

- A Key Performance Indicator (KPI) or Business Process Influencer (BPI) that could have a direct and negative impact to a company's "bottom line" if that KPI or BPI significantly missed a performance target.
- Most typically a BPI (a leading indicator) that must be identified after an in-depth analysis of the business process, versus a current KPI that is a lagging indicator.
- Can be quantified via different measures (e.g. days, percent, $, etc.)
- May or may not be unique to an industry, client-type or business process.

The First Orbit

- A PDP can be measured and monitored on a **Manual** (via a human interface) or **Real-time** (via a system output) basis.

The Second Orbit

- **Business Process** represents those discrete business processes that an organization wants to make more resilient.
- **Resource** defines into which one of the resource categories a PDP can be placed (i.e. **people, process, technology, network, data or facilities**.)

The Third Orbit

- **Threats** can be segregated into **environmental, supply, demand, process or controls**, and are typically, but not always, preceded by an event (e.g. event = earthquake, threat = tsunami).
- **Impact** represents the **financial ($), tangible or intangible impact** to the business should a threat materialize because of a preceding event thereby causing the Risk Atom to "move" from its stasis or equilibrium point through a performance threshold.

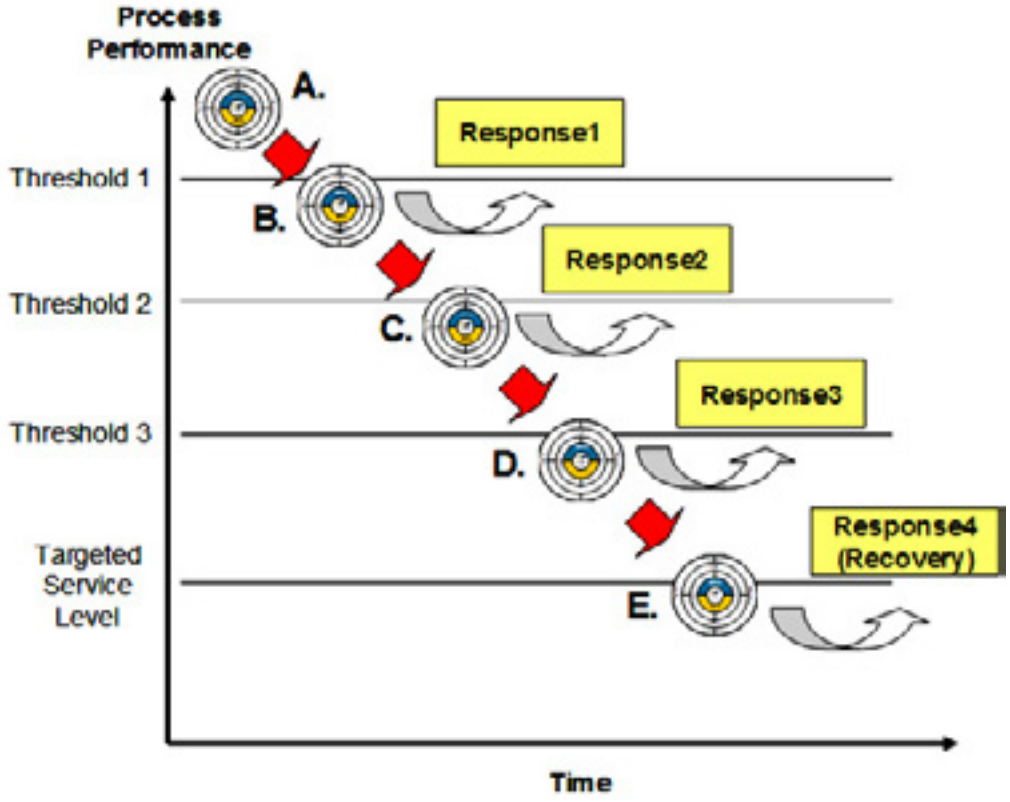
The Fourth Orbit

- **Response** defines the activities that a business must perform in order to respond to a manifested threat that causes the Risk Atom to "move" across performance thresholds over time.
- A response may be enacted to avoid, mitigate, transfer or recover from a particular situation and would encompass activities in one or all of the following areas: people, process, technology, network, data and facilities.
- **Risk Element** identifies those elements of the business that an organization wishes to "guard" in order to protect concepts such as customer goodwill, labor productivity, market capitalization or brand (for example) – things that could be irrevocably destroyed or have a severe impact on the organization's external standing in the business community if the organization was not prepared and/or resilient.
- A risk element may or may not be unique to a particular organization, and a single Risk Atom may encompass multiple risk elements.

1.4 Risk Atom Key Concept

Key to using the Risk Atom concept is establishing performance thresholds, which set parameters defining when targeted response activities are enacted. The risk atom key concept is movement through performance thresholds and is, illustrated in Figure 12.

Figure 12: Risk Atom movement through Performance Thresholds
(This figure does not show business impact by Threshold)
Note: 1) Thresholds are set in accordance with process needs
2) Threshold measures are user-selectable



Schematic of Figure 12 for risk atom and key concept is summarized as follows:

• A Risk Atom begins its journey at Point A – stasis or equilibrium.

• A threat impacts the Risk Atom and its performance measure drops until it passes Threshold 1 and finds itself at Point B. At that point the first response is activated in the hopes of potentially avoiding any further performance degradation to the business process.

• The Risk Atom continues to fall and passes through Threshold 2. At Point C the second response is activated in, an attempt to mitigate any impact from the threat.

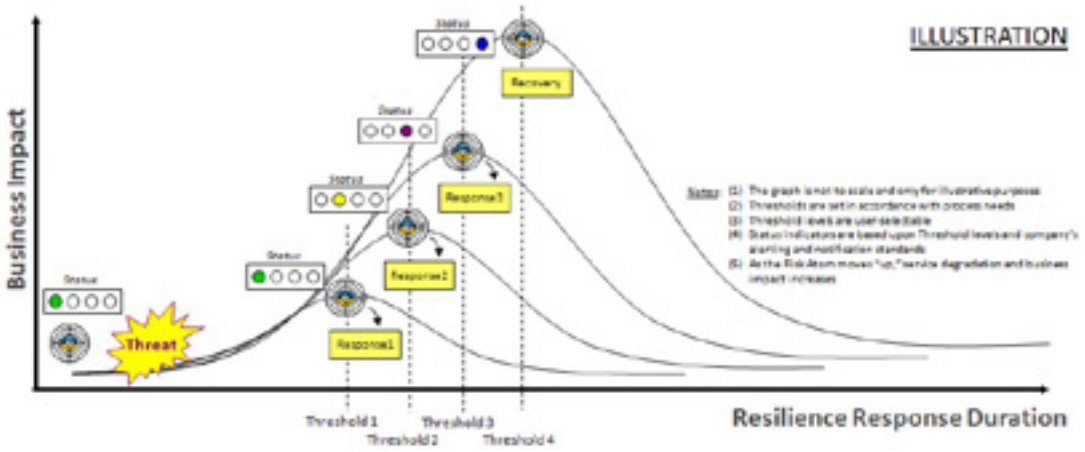
• The scenario continues to Point D where the third and final "resilience" response is activated.

• If the Risk Atom performance continues to fall towards the Targeted Service Level, the final response is to recover from the threat situation which means that the previous three responses did not rectify the fall of the Risk Atom and there could be a direct and negative impact on the company's "bottom line."

• The concept of a BRS Risk Atom is to provide and act upon threats before they critically, impact the business and cause potentially irreparable harm (i.e. become more resilient).

To reduce potential business impact and response duration, BRS helps drive proactive and timely response activities according to performance threshold levels. This is schematically illustrated in Figure 13 here.

Figure 13: Schematic of Resilience Response Duration



As part of our discussion in *Risk Atom*, we can summarize them here as:

• With BRS, the magnitude and duration of a disruption can be reduced as the business is receiving early warnings that a potential disastrous scenario could be imminent, and that targeted responses are being invoked to resume normal operations earlier in the degradation situation.

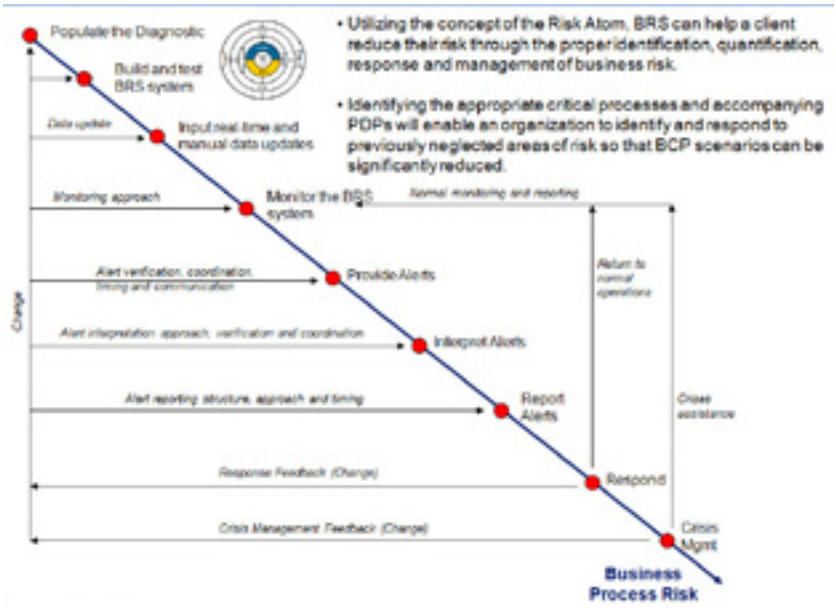
• The setting of thresholds allows the business to adequately, respond to a degradation situation before it becomes a disaster or destruction scenario.

• A Risk Atom will "move" because a manifested threat causes a degradation in the level of service that the Risk Atom represents.

• As a Risk Atom "moves," overall status may or may not change. For example, if the level of degradation is very small at Threshold 1, overall status may remain "green" and require simple monitoring of the situation. However, as the Risk Atom passes through the remaining Thresholds, failure to adequately, respond could drive the organization to recovery via the appropriate BCP thereby incurring significant impacts to the business and shareholder value.

From a functional process and system tool standpoint, BRS follows a linear track with the focus of reducing enterprise risk and increasing business resilience. This statement, is schematically - depicted in Figure 14.

Figure 14: BRS Functional Process and System Tool Standpoint

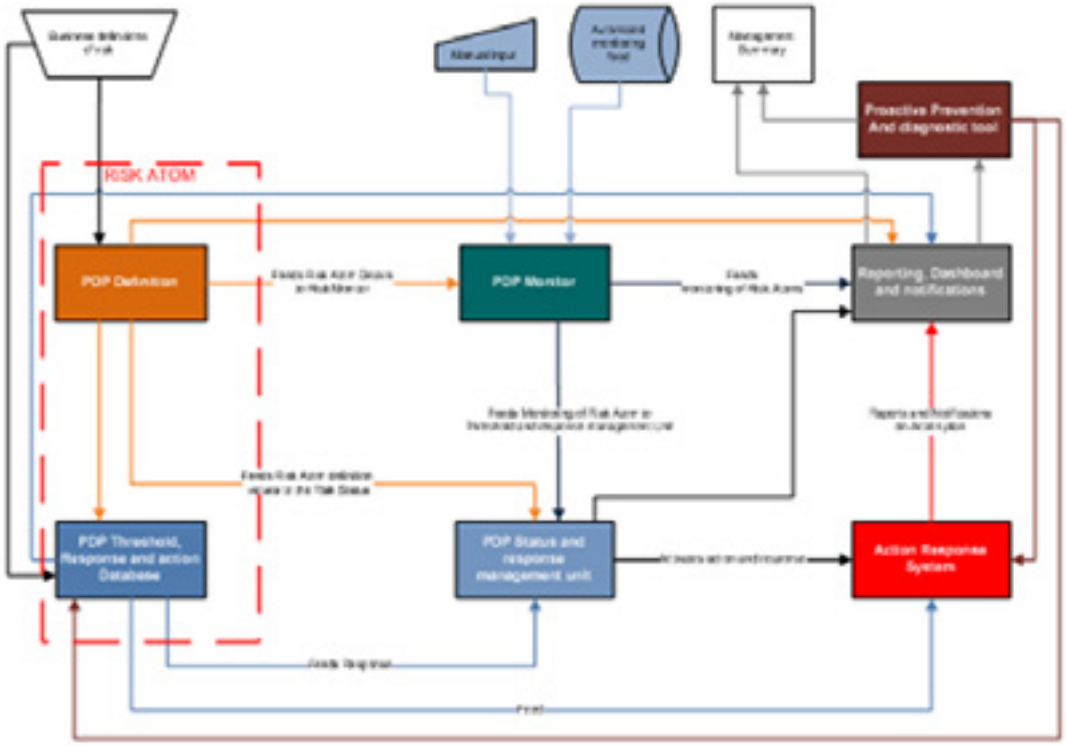


Using Fuzzy logics mathematical modeling to streamline the BRS risk management and business resilience approach, a high-availability toolset could be developed that suggests and consists of the following components:

- PDP identification, Threshold and Response Management database
- External and Internal monitoring of threats and events
- BRS Response Management Unit
- BRS Action response system
- BRS Dashboard and reporting system
- Proactive prevention and diagnostic tool

The above steps schematically are, depicted in Figure 15 here, which is presentation of BRS application architecture overview.

Figure 15: BRS Application Architecture Overview



As authors of this book, we are suggesting a holistic approach to simple, yet intelligent business resilience system, architecture configuration here. Of course, by no means this is a final and bulletproof approach. In today's computational technology along with autonomous functionality built on artificial intelligence and cloud computation availability and yet continuously thriving, a better and more robust system could be configured and designed. However, all futuristic BRS design will have one thing in common and that is the information that comes to them via PDP in Risk Atom Nuclei. For the PDP to be processed in real-time, wave of information and data via cloud computation should come in a very unidirectional or omni directional mode, if not real-time at least in near real-time basis. Considering the growth size of data in today's business, we certainly need to cut back on processing time of these data to be able to reduce them to some trusted values that PDP can process them and be able to send the notification to stakeholder and key decision maker in organizations and enterprises. By having, a very well thought trigging threshold point within dashboard of BRS system, per Service Level Agreement in place for the given application, alarming threats can then be identified. This way a measure can be taken with appropriate timeframe to counter the threat and react accordingly.

1.5 Business Resilience System Features

Business Resilience System (BRS) is a multi-featured application that is designed to use the latest available web-based technology with features such as:

- Highly configurable architecture
- Web-based risk definition and prioritization
- Web-based response management
- Document libraries with version control and document roll back
- Content publishing and online content authoring
- Real-time notification and collaboration
- Audit trail, reporting and custom dashboards
- Web-based Business Intelligence
- Work Flow engine and task coordination
- RSS (Rich Site Summary) feeds
- High end Search engine with inbuilt people search capability
- Pluggable authentication
- Integration with Office applications
- Policies auditing and compliance management
- Enhanced notifications – email, SMS (Short Message Service) and Voice
- Document and Folder level access control
- Mobile device support
- PDA (Personal Digital Assistant) devices

Some representative screen shots from an ideal BRS application are, shown in Figure 16 below:

To help analyze, define and implement a BRS solution, the BRS Functional Stack in Figure 17, will prove instructive as well as provide the project building blocks.

Figure 16: Representation of Ideal BRS Screen Shots

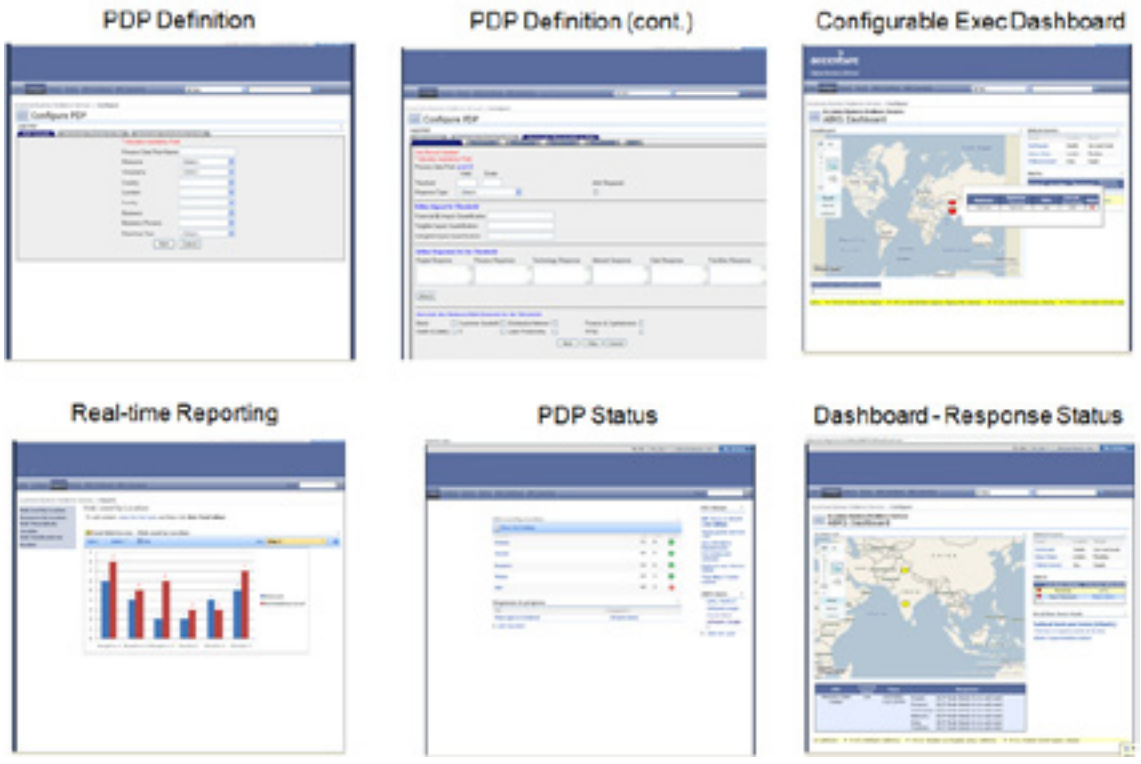
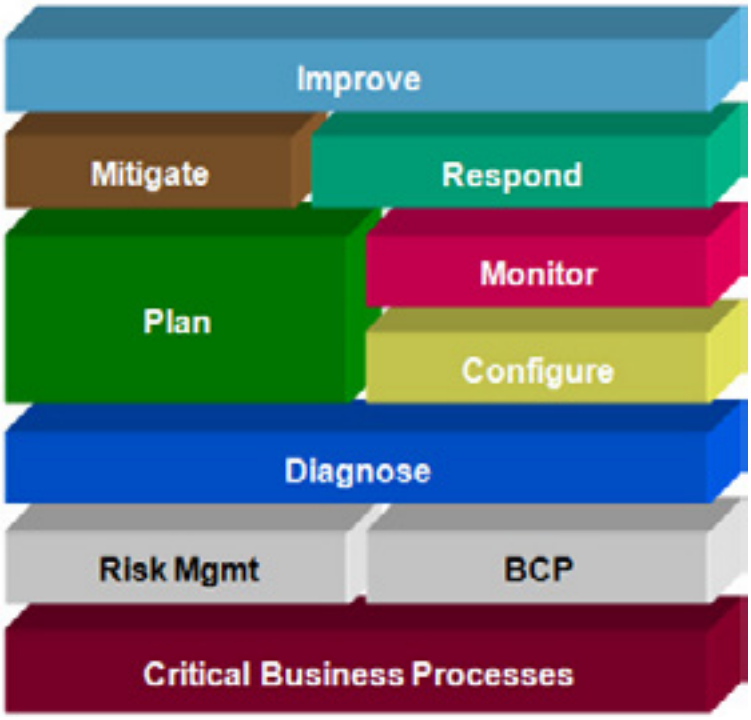


Figure 17: The BRS Functional Stack



The functional stack that is illustrated in Figure 17 is summarized below, with description of each element of stack.

• The footings for the BRS "stack" are an organization's current Critical Business, Risk Management and BCP processes.

• Enhancing these capabilities requires a diagnosis of the current process environment to identify, document and quantify the KPIs (Key Performance Indicators) and/or BPIs (Business Process Influencers) that have a direct impact on shareholder value.

• Following diagnosis, planning must be, performed to identify and develop appropriate threshold and situational responses as well as determine the degree to which any identified gaps from the diagnosis would be filled.

• Results from the diagnosis and planning steps would be, configured within the BRS tool to allow monitoring and presentation of threats, process/facility readiness, response activities, and external information data feeds.

• The next layer refers to the activities required within each resource set to mitigate the impact from a specific threat scenario. In turn, these are, assembled into appropriate responses based upon attained thresholds.

• As understanding of the organization's risk, response and mitigation capabilities matures, the BRS risk management and notification environment will be, continually improved.

Business resilience System (BRS) offering is briefly, illustrated in the Figure 18.

Identifying the correct Critical Business Processes (CBPs) to monitor and the Process Data Points (PDPs) that support them is the foundation of proactive business resilience and that is shown here in Figure 19 as well.

Functional Model of BRS Offering at top level where Fuzzy logic plays a major role is given in the following format as it can be seen in Figure 20.

BRS Portal Technology – Phase 1 to start with in order, to put the design of such system into action is schematically, offered here in Figure 21.

Business Resilience System (BRS) portal -- high-level system diagram is depicted in Figure 22 as follows. The technology overview as part of BRS offering feature is briefed here as follows;

Figure 18: BRS Offering

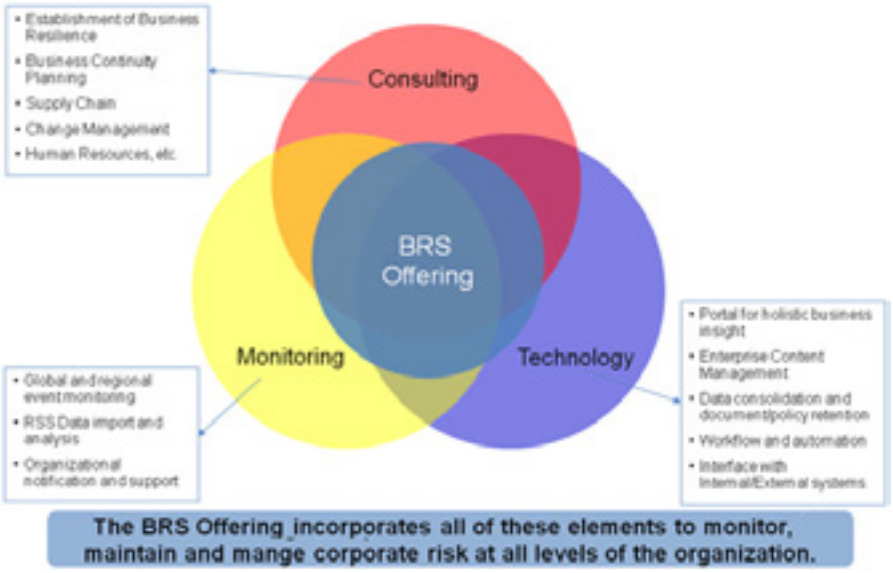
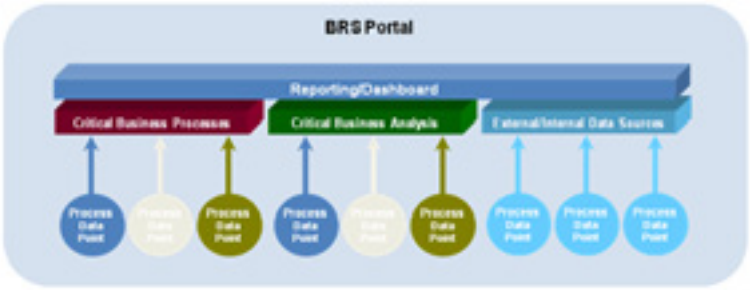


Figure 19: Illustration of Critical Business Processes

- The foundation of BRS is the organizations ability to identify the Critical Business Processes (CBP's) that support the organization or a particular component of the organization
- The Process Data Points (PDP's) that support these will be identified and thresholds and actions will be determined
- The PDP thresholds will be the basis for determining the appropriate reactive or proactive response that will need to be taken to mitigate or avoid the risk
- These thresholds can be changed or modified over time to optimize the response to meet the needs of the organization
- The PDP's and Critical Business Processes will be determined during the diagnosis and analysis processes

Figure 20: Business Resilience System Portal Configurations

The complete BRS offering then rolls in all of the CBP's and CBA's that need to be monitored and managed through a single portal.



- The portal becomes the business dashboard for executives to proactively manage their organization
- External and Internal Data sources (ERP, MRP, etc.) combined with the accumulation of CBP's and CBA's create a holistic view of business resilience

Figure 21: BRS Phase I Portal

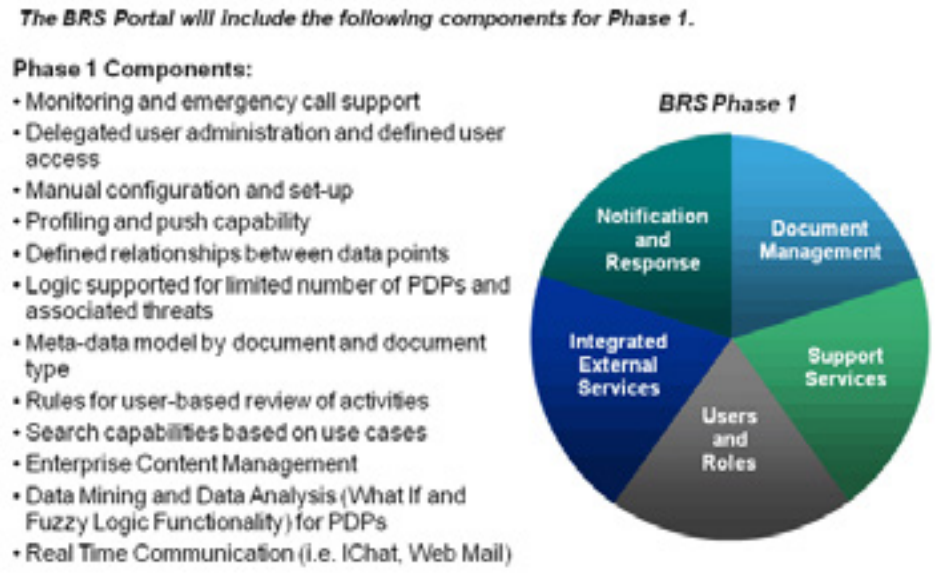
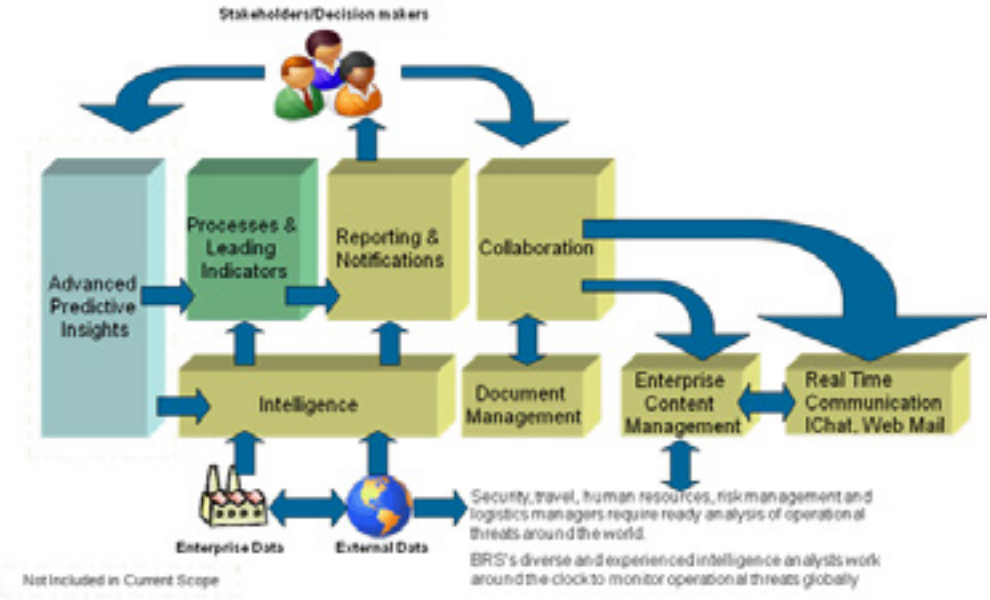


Figure 22: BRS Portal High Level System Diagram



❑ Crisis Preparedness

Crisis preparedness means knowing what to do and how to do it with a team that is practiced and ready. Safeway BRS (Business Resilience System) has particular expertise in developing policy, plan and procedures in support of corporate crisis management, supply chain risk management, expatriate risk management, and site emergency management. We also collaborate with leading risk consulting companies such as Marsh Risk Consulting and Kroll to deliver a comprehensive program tailored to each business specific needs.

❑ Integration Services

BRS can help you integrate data from your crisis / emergency management systems, employee data systems, and supply chain data systems as well as other related data systems (i. e., Tera-Data, Master Data Management).

❑ Implementation Services

BRS has successfully completed hundreds of complexes, client activation projects and refined the implementation process.

❑ **Special Projects**
BRS uses its extensive source network to produce detailed risk assessments and specialized intelligence on countries, cities and often, specific neighborhoods. Driven by each client's needs, these detailed intelligence reports range from on-the-ground crime, kidnapping and other security threats to geopolitical conditions, natural disaster, competitive business environments and transportation logistics.

❑ **Training Programs**
BRS offers a variety of specialized training programs that detail the travel security and safety issues that international travelers face, as well as the measures that corporate security, travel and risk professionals should take to ensure the safety of executives and corporate employees as they operate in the global marketplace.

❑ **Technology Approach**
BRS Approach is based on real and total web based solution utilizing. NET and J2EE as open source which is totally independent of OS clients for its implementation cross the internet and intranet.

Top 10 Questions to Think About
❑ Does our organization face rising Stakeholder and Shareholder expectations for its ability to sustain operations despite disruptive events?

❑ Does our company employ a comprehensive event response capability, using responses to routine disruptions to build skills and experience that will apply to disaster recovery?

❑ Have large or small disruptive events (e.g. blizzards, transit strikes, delivery delays, West Coast Port embargo, a power or network outage, computer virus, etc.) materially impaired your organization's delivery capability?
❑ Are "routine" disruptive events (e.g. - power outages, network down time, seasonal flu epidemics, hurricane evacuations, supply chain delays, etc.) considered part of "normal" operations not requiring a specific event response plan and capability?

❑ Have we analyzed our organization's annual quality and financial costs due to "routine" disruptive events?

❑ Can external events (e.g. regulatory changes, public panics) cause spikes or troughs in citizen demand for organization services? Does your organization have response plans for these disruptive demand changes? Would planning and preparation improve the organization's effectiveness in responding to such demand changes?

❑ Does our organization systematically monitor its environment for predictable, high-impact disruptive events, and have automated response capabilities in place to rapidly communicate status and begin response implementation?

❑ Have we established clear organizational accountability for our response capability?

❑ Do our organization's disaster recovery plans focus only on technology recovery or on full business capability (people, process, facilities, technology) recovery?

❑ Have our organization's operations (processing centers, call centers, etc.) quickly bounced back after Hurricane Katrina (or other hurricanes/disasters)? Are our clients even more dependent on your services during a disaster than during routine operations?"

1.6 Summary of Business Resilience System

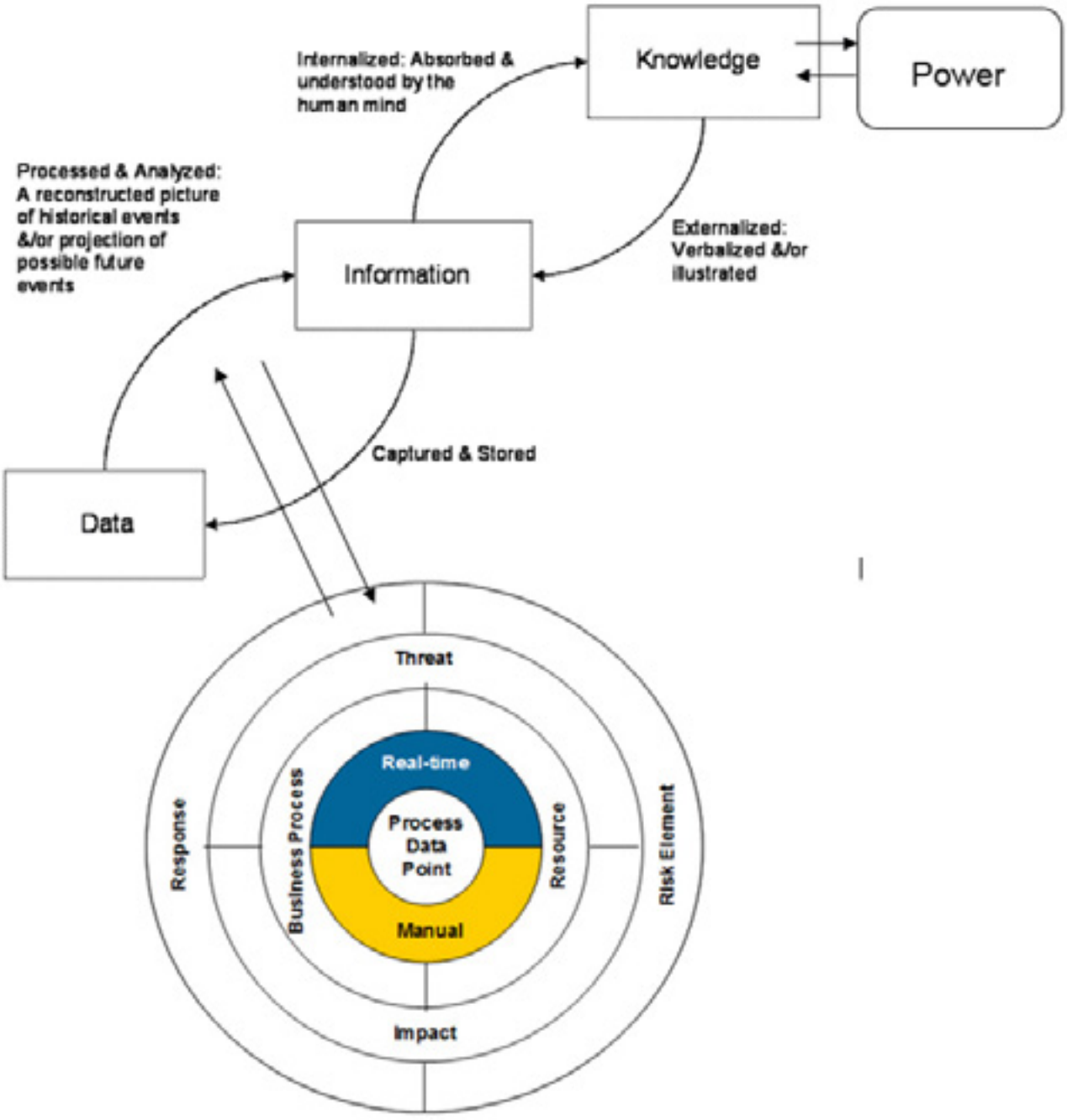
In summary Business Resilience System (BRS) is offering some type of system that is built around the best Artificial Intelligence (AI) concept and approach. Old saying that "Knowledge is Power) works perfectly, if our knowledge has real-time (at least near real) feed from vast data of information floating around us, and that comes to us from every direction providing that, we can trust them no matter what structure they possessed. For this AI machine to be in place and act autonomously as much as possible, float of data need to be continuous to its core of BRS Risk Atom, as we defined it Processing Data Point (PDP) in Figure 10. For this core to be actively and proactively to be effective and function properly against incoming cyber threats or any defined threat, building an intelligent model from data mining and expert knowledge is a must and inevitable. A look at some fundamental principles related to this matter is subject of next and following chapters. For a PDP to have an impact and effectively manage the 4 key orbits defined in Risk Atom, requires its capability to absorb the data processing driven either by Fuzzy or Boolean logic as part of its function and data mining, which is also subject later on chapters of this book.

For a stakeholder to have power of decision making to act up on an event of either adversary or productive for his/her day-to-day operation as an executive of an organization or enterprise, one need to have the knowledge. In order, to have knowledge, the same individual need to have information, where it comes from combination of data both structured and unstructured at Big Data level coming from omni direction 24 x 7 continually and the flow should be sustained without any interruptions.

However, for data to be useful and be on time for information gathering, we need to process them in real-time. Figure-1 is illustration 4-dimensioal cycle of such flow that shows the processing for the ultimate power.

As Figure-1 illustrates, data must be processed in real-time and requires a Risk Atom concept as demonstrated at lower part of Figure 2 to Figure 23.

Figure 23: Depiction of Data, Information, Knowledge is Power in Four Dimension



Bear in your mind that, the property that has given humans a dominant advantage over other species is not strength or speed, but intelligence. If progress in artificial intelligence continues unabated, AI systems will eventually exceed human in general reasoning ability. A system that is "super-intelligent" in the sense of being \ smarter than the best human brains in practically every field" could have an enormous impact upon humanity [7, 8]. Just as human intelligence has allowed us to develop tools and strategies for controlling our environment, a super-intelligent system would likely be capable of, developing its own tools and strategies for exerting control [8, 9]. In light, of this potential, it is essential to use caution when developing AI systems that can exceed human levels of general intelligence or that can facilitate the creation of such systems [10].

A business Resilience System also requires a true Incident Response Planning (IRP), to enable and preparing it for the inevitable threat or threats against organizations or enterprise that are using it, and to be to give enough warning to prepare the decision make and stakeholder for proper measures. Thus, as part of corporate internet security system, a "Computer Security Incident Response Planning" seems a fundamental requirement.

As we know, Computers and computer networks have been part of the corporate landscape for decades. However, it is only in the last five years that companies have started to connect these systems and networks to the outside world – suppliers, business partners, and the Internet. Unfortunately, in the hurry to get, connected and jump on the e-business bandwagon, computer security is frequently given short shrift, placing corporate assets at risk.

As an example of assets at risk, we can look at the media is filled with accounts of recent Internet security problems, including the denial of service attacks against Yahoo!, eBay, Amazon, CNN, and others, several instances of data theft involving credit cards or personal information, and the "I Love You" virus/worm. Although the press devoted many column-inches and on-air minutes to these stories, they focused primarily on the exciting topic of "the chase" to catch the perpetrators, and generally ignored the more important topics of how frequently computer security incidents occur, how many companies' data is at significant risk, and the potentially devastating impact of computer security incidents on their victims. A super smart Business Resilience System will provide a good and impenetrable line of defense to surround an organization or enterprise by providing advanced enough warning and put them ahead the ball.

In summary also, to help you determine if BRS may be right for your critical business processes or organization, 10 questions are, presented for your consideration as reader or folks that are interested in placing a more detail oriented BRS in place. These holistic questions were, imposed in above and we repeat it here again.

These holistic questions are:

ü Does your organization face rising Stakeholder and Shareholder expectations for its ability to sustain operations despite disruptive events?

 Does your company employ a comprehensive event response capability, using responses to routine disruptions to build skills and experience that will apply to disaster recovery?

 Have large or small disruptive events (e.g. blizzards, transit strikes, delivery delays, West Coast Port embargo, a power or network outage, computer virus, etc.) materially impaired your organizations delivery capability?

 Are routine disruptive events (e.g. - power outages, network down time, seasonal flu epidemics, hurricane evacuations, supply chain delays, etc.) considered part of normal operations not requiring a specific event response plan and capability?

 Have you analyzed your organizations annual quality and financial costs due to routine disruptive events?

 Can external events (e.g. regulatory changes, public panics) cause spikes or troughs in citizen demand for organization services? Does your organization have response plans for these disruptive demand changes?

 Would planning and preparation improve the organization's effectiveness in responding to such demand changes?

 Does your organization systematically monitor its environment for predictable, high-impact disruptive events? and have automated response capabilities in place to rapidly, communicate status, and begin response implementation?

 Have you established clear organizational accountability

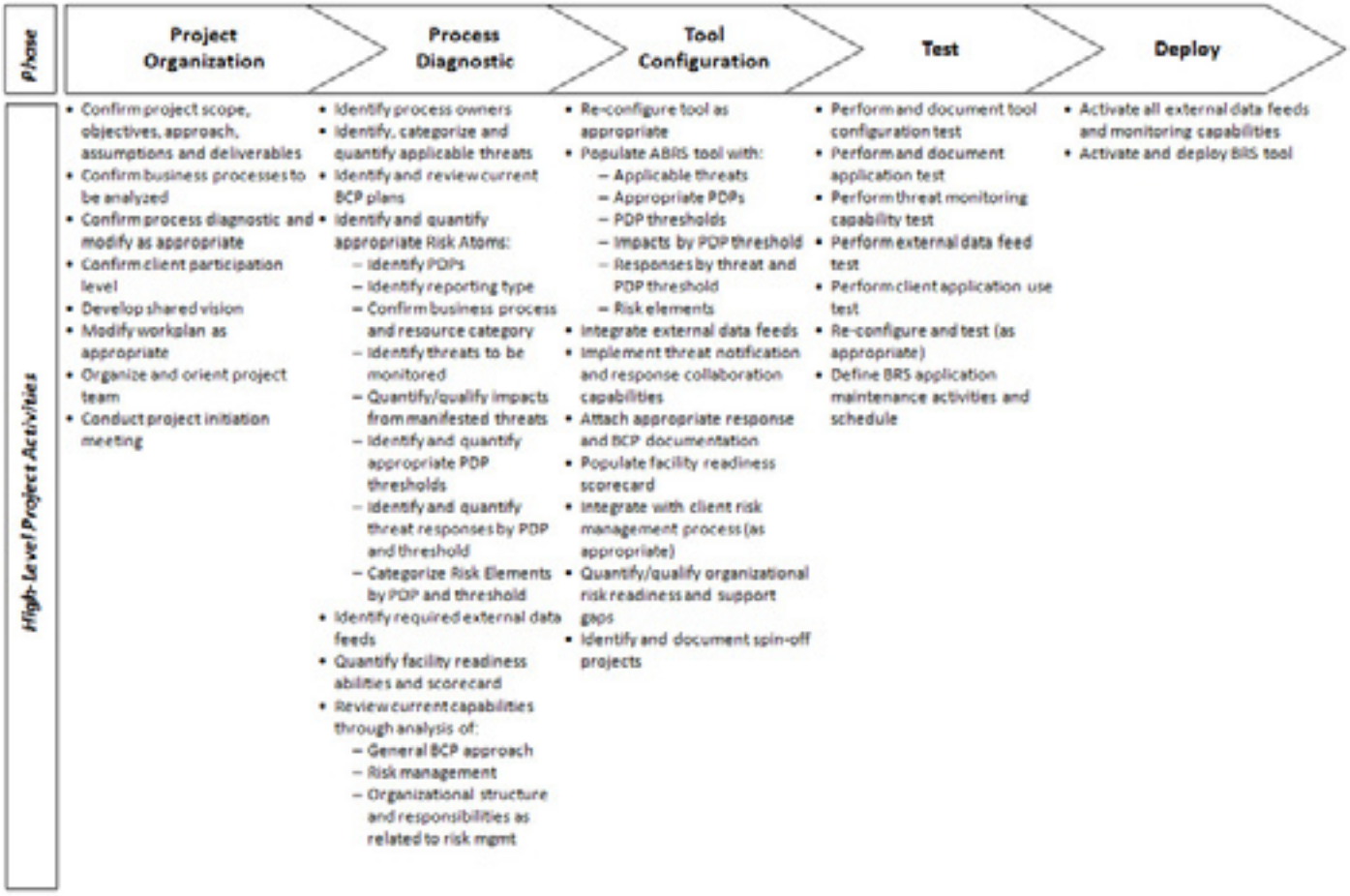
for your response capability?

 Do your organizations disaster recovery plans focus only on technology recovery or on full business capability (people, process, facilities, technology) recovery?

 Have your organizations operations (processing centers, call centers, etc.) quickly bounced back after Hurricane Katrina (or other hurricanes/disasters)?

 Are your clients even more dependent on your services during a disaster than during routine operations? Figure 24(a) and 24(b).

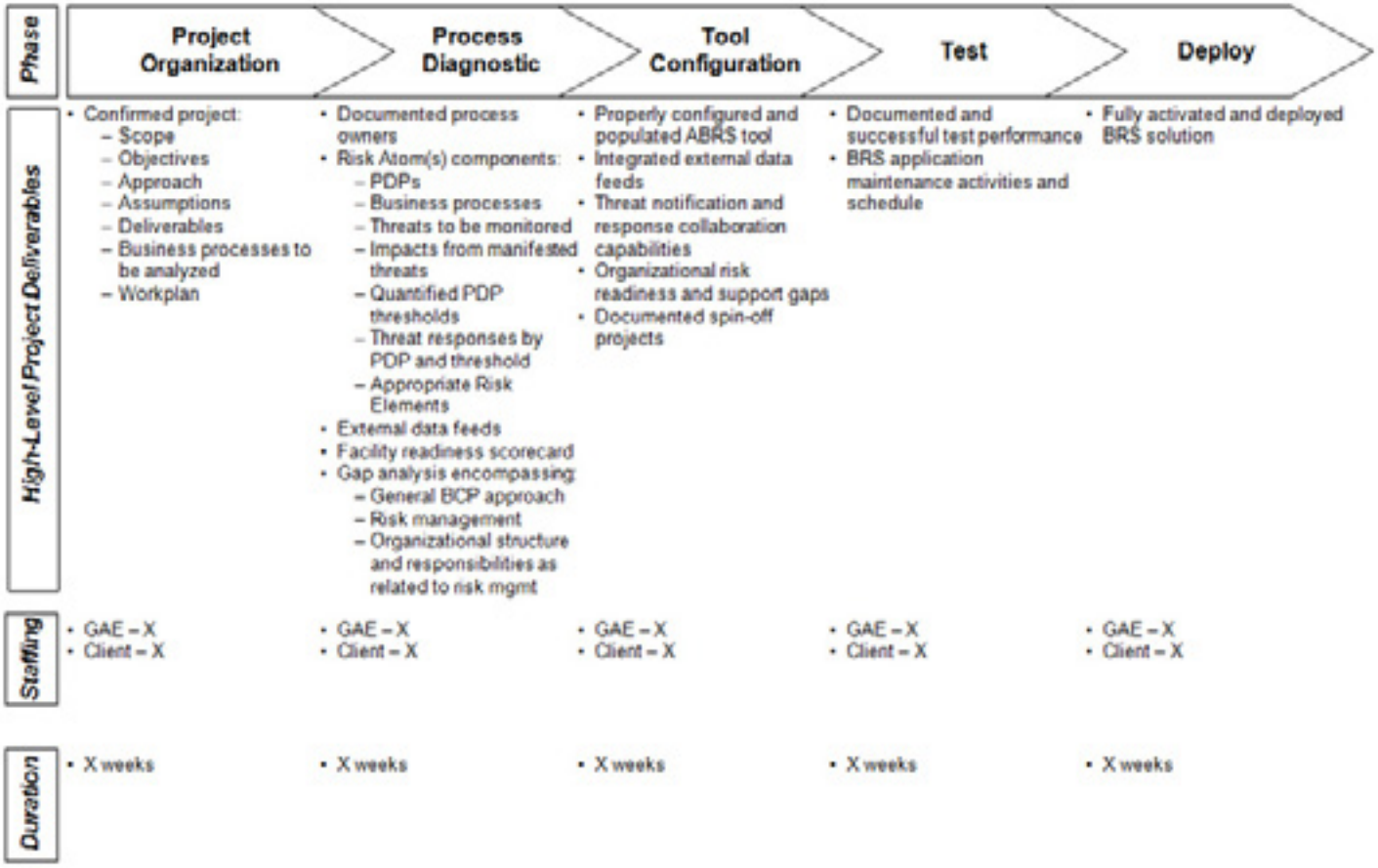
Figure 24(a): Illustration of a High-Level Project Plan



1.7 Summary of Business Resilience System

In summary Business Resilience System (BRS) is offering some type of system that is built around the best Artificial Intelligence (AI) concept and approach. Old saying that "Knowledge is Power) works perfectly, if our knowledge has real-time (at least near real) feed from vast data of information floating around us, and that comes to us from every direction providing that, we can trust them no matter what structure they possessed. For this AI machine to be in place and act autonomously as much as possible, float of data need to be continuous to its core of BRS Risk Atom, as we defined it Processing Data Point (PDP) in Figure 10. For this core to be actively and proactively to be effective and function properly against incoming cyber threats or any defined threat, building an intelligent model from data mining and expert knowledge is a must and inevitable. A look at some fundamental principles related to this matter is subject of next and following chapters. For a PDP to have an impact and effectively manage the 4 key orbits defined in Risk Atom, requires its capability to absorb the data processing driven either by Fuzzy or Boolean logic as part of its function and data mining, which is also subject later on chapters of this book.

Figure 24(b): Illustration of a High-Level Project Plan



Bear in your mind that, the property that has given humans a dominant advantage over other species is not strength or speed, but intelligence. If progress in artificial intelligence continues unabated, AI systems will eventually exceed human in general reasoning ability. A system that is "super-intelligent" in the sense of being \ smarter than the best human brains in practically every field" could have an enormous impact upon humanity [7, 8]. Just as human intelligence has allowed us to develop tools and strategies for controlling our environment, a super-intelligent system would likely be capable of, developing its own tools and strategies for exerting control [8, 9]. In light, of this potential, it is essential to use caution when developing AI systems that can exceed human levels of general intelligence or that can facilitate the creation of such systems [10].

A business Resilience System also requires a true Incident Response Planning (IRP), to enable and preparing it for the inevitable threat or threats against organizations or enterprise that are using it, and to be to give enough warning to prepare the decision make and stakeholder for proper measures. Thus, as part of corporate internet security system, a "Computer Security Incident Response Planning" seems a fundamental requirement.

As we know, Computers and computer networks have been part of the corporate landscape for decades. However, it is only in the last five years that companies have started to connect these systems and networks to the outside world - suppliers, business partners, and the Internet. Unfortunately, in the hurry to get, connected and jump on the e-business bandwagon, computer security is frequently given short shrift, placing corporate assets at risk.

As an example of assets at risk, we can look at the media is filled with accounts of recent Internet security problems, including the denial of service attacks against Yahoo!, eBay, Amazon, CNN, and others, several instances of data theft involving credit cards or personal information, and the "I Love You" virus/worm. Although the press devoted many column-inches and on-air minutes to these stories, they focused primarily on the exciting topic of "the chase" to catch the perpetrators, and generally ignored

the more important topics of how frequently computer security incidents occur, how many companies' data is at significant risk, and the potentially devastating impact of computer security incidents on their victims.

A super smart Business Resilience System will provide a good and impenetrable line of defense to surround an organization or enterprise by providing advanced enough warning and put them ahead the ball.

In summary also, to help you determine if BRS may be right for your critical business processes or organization, 10 questions are, presented for your consideration as reader or folks that are interested in placing a more detail oriented BRS in place. These holistic questions were, imposed in above and we repeat it here again.

These Holistic Questions are:
Does your organization face rising Stakeholder and Shareholder expectations for its ability to sustain operations despite disruptive events?
Does your company employ a comprehensive event response capability, using responses to routine disruptions to build skills and experience that will apply to disaster recovery?
Have large or small disruptive events (e.g. blizzards, transit strikes, delivery delays, West Coast Port embargo, a power or network outage, computer virus, etc.) materially impaired your organization's delivery capability?
Are "routine" disruptive events (e.g. - power outages, network down time, seasonal flu epidemics, hurricane evacuations, supply chain delays, etc.) considered part of "normal" operations not requiring a specific event response plan and capability?
Have you analyzed your organization's annual quality and financial costs due to "routine" disruptive events?
Can external events (e.g. regulatory changes, public panics) cause spikes or troughs in citizen demand for organization services? Does your organization have response plans for these disruptive demand changes? Would planning and preparation improve the organization's effectiveness in responding to such demand changes?
Does your organization systematically monitor its environment for predictable, high-impact disruptive events? and have automated response capabilities in place to rapidly, communicate status, and begin response implementation?
Have you established clear organizational accountability for your response capability?
Do your organization's disaster recovery plans focus only on technology recovery or on full business capability (people, process, facilities, technology) recovery?
Have your organization's operations (processing centers, call centers, etc.) quickly bounced back after Hurricane Katrina (or other hurricanes/disasters)? Are your clients even more dependent on your services during a disaster than during routine operations?"

References

1. GEOG 30N (2011) Geographic Perspectives on Sustainability and Human-Environment Systems.

2. Holling AS (1973) Resilience and Stability of Ecological System, Annual Review of Ecology and Systematic 4: 1-23.

3. David DW, Erik H (2006) Resilience Engineering: Concepts and Precepts CRC Press.

4. Rasmussen J (1997) Risk management in a dynamic society: a modelling problem Safety Science 27: 183-213.

5. Fei-Yue, Wang, Liu D (2008) Networked Control Systems: Theory and Applications.

6. Karl E Weick. 2018, Wikipedia.

7. Bostrom Nick (2014) Superintelligence: Paths Dangers Strategies.

8. Muehlhauser L, Anna S, Johnny S, et al. (2012) Intelligence Explosion: Evidence and Import. In Singularity Hypotheses: A Scientific and Philosophical Assessment.

9. Nate S, Benya F (2017) Agent Foundations for Aligning Machine Intelligence with Human Interests: A Technical Research Agenda.

10. Zohuri B and Moghaddam M (2017) Business Resilience System (BRS): Driven Through Boolean Fuzzy Logics and Cloud Computation: Real and Near Real Time Analysis and Decision-Making System.

Citation: Bahman Zohuri (2018) A General Approach to Business Resilience System (BRS). SF J Artificial Intel 1:3.