International Conference and Utility Exhibition 2014 on Green Energy for Sustainable Development (ICUE 2014)
Jomtien Palm Beach Hotel and Resort, Pattaya City, Thailand, 19-21 March 2014

General Resilience: Taxonomy and Strategies

Hiroshi Maruyama, Roberto Legaspi, *Member, IEEE*, Kazuhiro Minami, and Yoshiki Yamagata

***Abstract*-- Because resilience thinking has increasingly been used in various disciplines and domains and extended with a broader scope of concepts, it is difficult to find a unified and encompassing definition by which it can be accurately referred to. Furthermore, to elucidate and synthesize all resilience theories and conceptual frameworks that have been put forward will require volumes of written work. We therefore argue in this paper that research works pursuing the common strategies of system resilience require a language that can help describe the specific contexts in which resilience is applied. We propose here a taxonomy for general resilience that consists of four orthogonal dimensions, namely, type of shock or perturbation, target system, phase of concern, and type of recovery. Furthermore, it has also been observed that despite its domain-dependency, there exist resilience strategies that cut across multiple disciplines and domains, specifically, redundancy, diversity and adaptability. There is another, however, which we argue here in detail that is equally compelling, i.e., a strategy that can break the rigid stability that leads to greater fragility and a more severe collapse with prolonged period of severity. Specifically, the strategy is to deliberately inject or induce regularly small "controlled" shocks into the system to regulate the build-up of complexity and rigidity among its components and their connections. Doing so will not only prolong the period of stability of the system, but also shorten the period of severity in the wake of a severe shock.**

***Index Terms*-- Nonlinear systems, Resilience.**

I. Introduction

After the massive devastation brought about by the earthquake off the Pacific coast of Japan's Tōhoku region – the earthquake often referred to as "*3.11*", there has been a significant increase in the number of discussions on events that can have massive impact and can catch us off guard. These events are characterized in the literature as rare and unforeseen [20], unprecedented, ill-defined [12], multiple-sigma [19], noncomputable surprise [13], and referred to as Black Swans [47] or X-events [14]. In the wake of 3.11, for example, the town of Miyako in Iwate experienced waves that reached up to 40.5 meters high[1], which was way beyond the anticipated maximum of 5.6 meters. These events do happen and are inevitable, which implies that it may not all be possible, theoretically or practically, for us to completely shield all our *systems* that keep our humanity and lifestyle, as well as our world, existing and flourishing. When a system fails, the tendency should be to recover from the damage as promptly and inexpensively as possible. This process may not be a recovery per se since the system may be restored, not to its original configuration or form, but to something completely new that is acceptable or even desirable. The ability of a system to withstand large perturbations and enable *generalized* recovery once it fails is what we refer to as *resilience*.

To shed scientific light on the concept of resilience, we started in April 2012 our multi-year multidisciplinary project, called *Systems Resilience*[2] [36], within the auspices of the Transdisciplinary Research Integration Center of the Research Organization of Information and Systems[3], which is a national research organization under the Japanese Ministry of Education, Culture, Sports, Science and Technology. Our goal is to investigate the common set of strategies that make a system resilient regardless of its domain and to catalogue these strategies into a body of knowledge that describes when and how the strategies should be applied. This body of knowledge is therefore aimed to support a scientifically accountable, sound and well informed decision making process when designing our systems to be resilient. While we fully recognize the fact that resilience thinking has been around for a while now, most certainly in the fields of psychology [39][37] and ecology [24][22], and has been extended to wider areas of applications (e.g., power grids in engineered systems [45] and disaster prevention and recovery in social systems [42][43], among many others), we are also cognizant of the fact that there is no explicit unified and encompassing definition or concept to which it can be accurately referred to. Furthermore, to elucidate and synthesize all the theories that embed it and conceptual frameworks that embody it will require volumes of written work [35]. We therefore argue in this paper that to communicate the diverse concepts that elucidate the various strategies for general resilience requires a taxonomy.

Despite its domain-dependency, however, there exists certain resilience strategies that cut across multiple disciplines and domains. One strategy that is compelling and specific to our study is to break the rigid stability that leads to greater fragility and a more severe collapse with prolonged period of severity [24][27][34][46][51]. When the parts of the system become more complex and even more connected, albeit stable, the more it reduces its capacity to cope with the severe adverse, let alone rare and unprecedented, events. Hence, we

H. Maruyama, K. Minami, and R. Legaspi are with the Research Organization of Information and Systems, The Institute of Statistical Mathematics, 10-3 Midori-cho, Tachikawa, Tokyo 190-8562, Japan (e-mails: {hm2, kminami, legaspi.roberto}@ism.ac.jp).

Y. Yamagata is with the Center for Global Environmental Research, National Institute for Environmental Studies, Onogawa 16-2, Tsukuba, 3058506, Japan (e-mail: yamagata@nies.go.jp).

[1] http://ajw.asahi.com/article/0311disaster/quake_tsunami/AJ201106030393
[2] http://systemsresilience.org/index-e.html
[3] http://www.rois.ac.jp/english/

also argue in this paper that resilience does and should include extending the period of stability, but also evading a prolonged period of severity in the wake of a severe shock. The specific strategy is to deliberately inject or induce regularly small *controlled* shocks into the system to regulate the build-up of complexity and rigidity among its components and their functions and connections. We qualify "controlled" here to mean timely and with the right dose, regardless of whether the shock is inflicted by man or comes by the natural law of things.

The rest of the paper is written as follows. The succeeding section elucidates in detail our proposed taxonomy for general resilience. Section III discusses the resilience strategies we have found consistent across disciplines and domains, and how we map these general strategies to our taxonomy. Section IV details the strategy of introducing controlled shocks. We conclude with our recap and a hint to our next step.

II. TAXONOMY OF RESILIENCE

Resilience is context dependent. This means that the strategies that made life on earth survive for billions of years can be much different from what makes life today resilient against various kinds of perturbations. Hence, when we talk about resilience, we need a language that can describe its context. We detail in this section the four questions that are indicative of the *dimensions* of our taxonomy for describing resilience in various contexts.

A. From Questions to Dimensions

1) Resilience to What? – Type of Shock

We consider first the types of shock systems may encounter. There are several sub-dimensions regarding the perturbation:

Cause (natural or intentional). The shock may originate from a natural phenomenon, e.g., earthquakes, strong typhoons, and tsunami, which occur randomly according to some statistical distribution. Other shocks may be intentional, such as war, cyber-attacks, and terrorism (e.g., various relevant and compelling real incidents discussed in [20]). These events are less random, because intelligent originators choose for their attack the most vulnerable parts of the system at the time it is most vulnerable. For example, it is known that scale-free networks such as the Internet is very robust against random failures but vulnerable to elaborate attacks to its weakest points, e.g., the root DNS servers [7].

Frequency. The shock can be very frequent. For example, an average of more than 1.24 million people were killed in traffic accidents in 2010 according to WHO[4]. Other shocks are very rare. Multiple sigma (σ) is at times used to indicate the low probability of occurring, e.g., the occurrence likelihood of 4-σ and 5-σ events correspond to less than 0.01% and 0.000057%, respectively [19]. A meteor impact of more than 1,000 mega-tons of energy occurs every 10,000 to 100,000 years[5]. The point, however, is that while frequent shocks can be anticipated more, hence can be prevented more, through some means (e.g., traffic lights), preparing for an extremely rare event, on the other hand, is plausibly impossible or too costly. If an event is rare, then recorded observations are scarce, data to fit models are sparse, and consequently, to construct knowledge from useful trends to probability models is difficult [12]. Investing therefore on recovery more than prevention makes more sense in the latter.

Level of anticipation. Some shocks are predictable. For example, the National Weather Service in the US and the Japan Meteorological Agency can provide very accurate hurricane or typhoon warnings a few days prior to landing. If reliable prediction is possible, the system can change mode (e.g., evacuate coast-line residents) to prepare for the event. On the other hand, current state-of-the-art technologies may still fall short in accurately predicting the exact time and location of large earthquakes. Due to the inadequacies of anticipative warning mechanisms, preparation is not an optimal option when it comes to unpredictable adverse events.

Time scale. Some shocks are instantaneous, such as lightning and earthquakes. Responding to these acute events while they are on-going is difficult. Other shocks are chronic, i.e., their existence from start to finish is longer (e.g., global warming), which implies that we have enough time to analyze the shock it brings and make plans on how to respond. Note, however, that responding to acute shocks is difficult but not impossible given the premise that, still, they occur in a finite amount of time (e.g., a typical lightning travels at the speed of 6,000 km/sec). Hence, if the system can detect the beginning of the event and has the mechanism to respond quickly enough, then the response strategy may well work.

Source (external or internal). Many shocks, such as natural hazards, come from outside the system, but some are internal. Per Bak and his colleagues showed through their famous sand pile model that a system that gets larger and more complex will eventually collapse because of its "self-organized criticality" [5][6]. The financial crisis in 2008 is a typical example of an internal collapse. In their book, Zolli and Healey detailed how the big complex and shady connections among banks made the entire system so ready for collapse [51]. The collaterized debt obligations and credit default swap tools were meant for the market to benefit those who are willing to take risks on investments and allow banks to mix-and-match their activities with other banks (e.g., originate or buy from others its mortgages, sell mortgages, insure another bank from default, etc.). But with these activities, through the years unregulated and with no outside intervention, the bank institutions eventually found themselves entrenched into highly complicated connections to a point that it was impossible to know who had a contract with whom and which contracts had the potential for catastrophe. The derivative contracts, for example, were so complicated that one contract may ran from

[4] See http://www.who.int/gho/road_safety/mortality/en/.

[5] http://www.nature.com/nature/journal/v420/n6913/full/nature01238.html

a few hundreds to an excess of one billion pages, hence, anybody would just conveniently take in the contract of the other bank. Lehman, Bear Stearns and AIG, the very banks that were "too big to fail", were the very ones who had such connections of indeterminable size and granularity.

2) Resilience of What? – Target System

The second question pertains to the system itself that needs to be resilient to perturbations:

Domain. What was once contained within the bounds of natural systems, resilience thinking has been extended to a wider scope of features, or as other research works put it, principles, conditions, strategies, or capacities that are applicable to different kinds of systems [35], including ecological [24][22][18], biological [4][32], economic [9][28], financial [21], engineering [26][50], community [42][43][10], organizational [3], and of course, human developmental [37][38], among others. Systems can also be viewed in relation to other systems, as in system-of-systems or linked systems, e.g., in socio-ecological-economical [22][23][25][49].

Granularity. Resilience may refer to the ability of an *individualized* system. Psychologists have long studied how some individuals were successful in recovering from the traumatic events of the Holocaust while other people were not (e.g., [39], and in [51]). The word resilience in psychology is used in this context. Other systems consist of a *group* of individuals with the same make-up. For example, when we discuss the resilience of a community, the focus extends beyond the individuals of the community towards the survivability of the community as a whole (e.g., [42][43]). At the loss at times of a small portion of its individuals, albeit fatal and tragic, the community at large could continue to exist, and thus, is considered to be resilient. The last case is that of the system consisting of multiple *species* or *types*, e.g., the ecosystem. A loss of a small number of types (species) can be tolerable, or even desired, for the resilience of the entire system, as in the case of the ecosystem's evolution where loss of some species can create a room for new innovative species.

Passive vs. Active. Some systems are autonomously resilient, i.e., their resilience is native or built within. Take for example the reverse evolution of the armor plates of the three-spine stickleback as reported by Kitano and his colleagues [32]. In 1957, a sample of this species was caught in Lake Washington and was observed to have no armor plates. Recent samples, however, had been observed to possess armor plates. One theory to explain this is that as the three-spine stickleback lost their armor plates when they migrated from sea to fresh waters some 10,000 years ago, the species regained the plates back because of the predation pressure imposed by the increase in the trout species population during the period when the transparency of the water in the lake increased. We call this capability of autonomous recovery as *passive* resilience.

Other systems involve human intelligence, and what Zolli and Healey calls cognitive diversity [51], in their feedback loop. For example, companies have to deal with external shocks such as financial crises and new competitors. Their response is not automatic and usually requires elaborate analysis and careful planning. Another example is a community-based renewable electricity sharing system where the collective dynamics of a community can come into play as members collaborate to partake of the available renewable electricity in the event that a major disaster brought down the electric power grids [10]. One key aspect to note here is that this process permits creativity and innovation, as products of human intelligence at work and by collaboration among cognitively diverse individuals, to emerge and flourish. We use the term *active* resilience when human intelligence is involved.

Function (or utility). Some systems have a clear objective. For example, the performance of a company is measured by one or relatively small number of well-defined metrics such as total revenue, net profit, earnings-per-share and market value. For these systems, resilience could be defined by Bruneau's Triangle [11] (shown in Fig. 1) that represents the loss of a system's functionality and the duration of this loss due to shock and the pattern of system recovery over time.

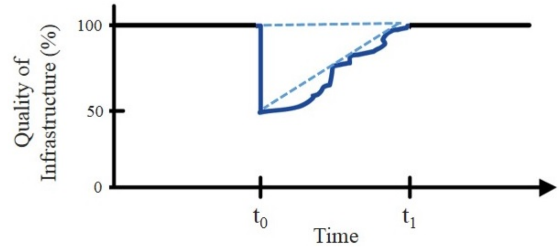


Fig. 1. The resilience triangle given by Bruneau as a measure of the concept of seismic resilience.

In other systems, however, the objective function can be obscured and usually involves multiple stakeholders. After the Great East Japan Earthquake hit Japan, there had been a lot of debates among many stakeholders on the priorities of the recovery operations [8].

3) Resilience at What? – Phase of Concern

The third question to ask, especially when talking about resilience strategy, is at which phase of resilience is a particular strategy applicable. Fig. 2 shows our own view of a resilience cycle with its seven different phases.

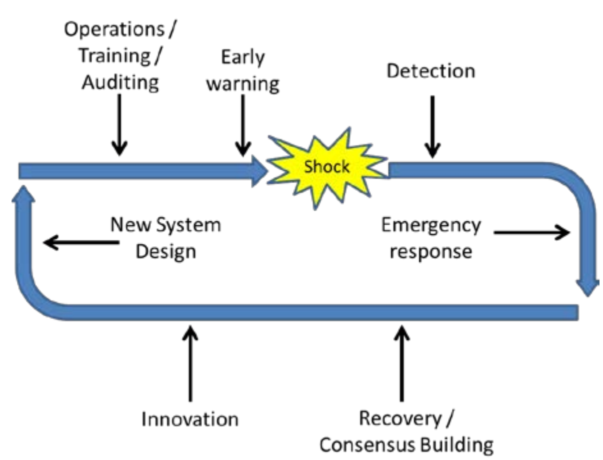


Fig. 2. Resilience strategies focus on different phases of resilience.

Design time. Many resilience strategies are intrinsically built into the system design. Computer systems have a certain level of redundancy in their design, e.g., the RAID, which stands for Redundant Array of Inexpensive Disks, are used by mission-critical storage systems so that functions can continue even though one or more disks fail [40]. The DNA mechanism in biological systems has very robust reproduction capability in its design, although this design is not an intentional byproduct of any intelligent entity, whether human or artifact.

During daily operations. Operating policies and procedures are important to maintain system functionality and readiness for perturbations. Best practices in IT management, for example, are defined as international standards, such as ITIL[6], COBIT[7], and ISO 27001 for computer systems [29]. These operating procedures include training (e.g., fire drills) and periodical self-checks or third-party auditing.

Early warning. If the shocks are predictable, investing on early warning systems (e.g., supercomputers for weather forecasting) and associated countermeasures (e.g., evacuation procedures) make the system more resilient.

Detection. Shocks need to be detected before the system can take any responsive actions. The earthquake detection network in Japan is very sophisticated and was able to detect the Great East Japan Earthquake quickly enough for all the bullet trains in operation to be stopped or slowed down before the main wave of the earthquake hit the tracks. This detection network saved thousands of lives.

Emergency response. Some resilience strategies are concerned at emergency time. Fire shutters automatically close in case of fire and compartmentalize the system so that the damage is contained. The Emergency Core Cooling System (ECCS) of a nuclear power plant injects water to safely shut down the reactor.

Recovery. Once damages are inflicted, the system has to recover from them. After the supply chain of Toyota Motors was severely damaged due to the 3.11 earthquake, they quickly rebuilt the supply chain by allocating alternative sources [8].

Recovery planning is sometimes not straightforward because there are multiple stakeholders and they may not agree on the priorities. How to make decisions during recovery operations can be discussed and agreed upon in advance.

Innovations. A loss of some portion of the system may present an opportunity for the system to innovate. In the aftermath of the Kobe Earthquake in 1995, many old wooden houses were destroyed, but the city reappeared as modern, efficient, and with much safer complex of apartment buildings.

This resilience cycle goes back to the new system design, which will be implemented and operated until the next major shock that necessitates going through another recovery, innovation, and new system design phases. From this viewpoint, we consider a system *resilient* as long as this cycle continues and the essence, or the “core” (we shall go back to this and explain further), of the system is preserved.

[6] http://www.itil-officialsite.com/home/home.asp.
[7] http://www.isaca.org/COBIT/Pages/default.aspx.

Note that even though the names of the phases defined above are chosen from the perspective of managing man-made systems, the ideas can also be applied to natural systems, e.g., animals have early warning on, detection of, and/or response capabilities to, common threats.

4) Resilience of What Kind? – Nature of Resilience

As we have put forward early in this paper, our definition of resilience pertains to the ability of a system to withstand shocks and enable an efficient and effective generalized recovery. Hence, the last dimension that concerns us is the varied-level recovery that is needed.

Structural resilience. If the system needs only to recover to its original structure and workings, then we call it *structural* resilience. One concrete example are the many fault-tolerant or robust engineering systems that preserve structural identity simply by replacing the damaged parts with new ones, but of the exact same type. This means that the system is able to absorb the impact of the shock and remained unchanged, with its form and operations, or not permanently damaged. This implies that the recovery is quicker because the system components can be segregated from the other interacting parts, i.e., are modularized, to be restored or returned to normal.

Functional resilience. In some cases, the system can change its structure as long as its functionality is preserved. Toyota’s supply chain had been changed after the earthquake, but the company’s overall objective, i.e., to produce quality autos, is preserved. We call this *functional* resilience.

Core resilience. In some extreme cases, a system is considered to be resilient even if it loses its original structure and functionality and is reborn with a new set of configurations and objectives, but not losing the integrity of its very nature and essential. The Japanese Empire, for example, even though it was almost completely destroyed in 1945, emerged to a new democratic nation with new values, namely, freedom and democracy. Although the people in Japan experienced painful moments during the war, Japan has recovered and prospered more than the time prior to the war. We call this *core* resilience.

B. Proposed Taxonomy

We synthesize in Table I (refer to the next page) the various aspects embedded in the above four questions. Any resilience research can be characterized by marking the appropriate position in each dimension and sub-dimension. We believe that this taxonomy can help communicate ideas regarding various strategies for general resilience.

III. General Resilience Strategies

In our aim to construct a common language that will help describe resilience that cuts across disciplines and domains, it is inevitable that we compile a set of strategies that can enable or support general resilience. So far, we have compiled four – the first three will be mentioned in this section, while the last is elucidated in detail in the succeeding section.

We described in an earlier paper [36] resilience strategies that have been observed as common to different systems,

TABLE I
TAXONOMY FOR RESILIENCE

1]	Type of Shock	Cause	Natural	←- - - - - - - - - - - - →			Intentional
		Frequency	Frequent	←- - - - - - - - - - - - →			Rare
		Anticipation	Predictable	←- - - - - - - - - - - - →			Unknown unknown
		Time Scale	Acute	←- - - - - - - - - - - - →			Chronic
		Source	External	←- - - - - - - - - - - - →			Internal
2]	Target System	Domain	Biology	Engineering	Financial	Legal	Civil Infrastructure
				Organization	Community	Society	
		Passivity	Passive	←- - - - - - - - - - - - →			Active
		Granularity	Individual		Single Type		Multiple Type
		Objective	Simple	←- - - - - - - - - - - - →			
3]	Phase of Resilience		Design Time	Operations	Training	Evaluation	Early Warning
			Detection	Emergency Response	Recovery	Consensus	Innovation
4]	Type of Resilience		Structural		Functional		Adaptive

namely, redundancy, diversity and adaptability. We shall now demonstrate that the taxonomy defined in the previous section helps understand how these strategies can be most effectively applied within a given context and how they are interrelated.

A. Redundancy

First, the redundancy – of organisms, functions, knowledge or skills, for example – contributes to the recovery from shocks. Biological systems are known to have a large redundancy. Interesting, for example, is the case of the E. Coli that has approximately 4,300 genes, but with almost 4,000 of them known to be redundant. This means that damaging one of them will not deter its ability to reproduce [4].

Redundancy is a simple strategy frequently seen in situations where the shocks are relatively well-known and frequent, such as failures of hardware parts. Redundancy in its simplest form keeps the structural identity of the system, i.e., the redundant parts addresses the same purpose. This does not mean, however, that the parts in reserve cannot be designed to be general-purpose, or at least multi-purpose, so that the system may have a different configuration upon recovery.

B. Diversity

Research have found that ecosystems with species diversity (i.e., it is species-rich) [33][41][44], functional diversity (i.e., consists of different kinds of processes) [44][17], or response diversity [18] (i.e., possessing similar functions, hence, with higher susceptibility to threats or to changes), have species that can exploit more efficiently the resources they need and preserve more effectively their functions even if some of their components are damaged [18]. The survival of biological systems as a whole, even with seemingly unfathomable crises that endangered their survival for millions of years, can be attributed to species having had different capabilities to deal with changing environments.

Diversity is usually a costly strategy compared to redundancy, e.g., having a back-up system of the same design is less costly than having a back-up system with a different design. However, when the shock is completely unknown, i.e., there is failure in anticipating extreme environmental parameters in the design, diversity plays an important role. Note that in certain contexts diversity does not work effectively. For example, if the system in question is a single individual, it is impossible to have diversity in that level. But this does not mean that we cannot discuss the diversity when it comes to the components of this system.

How to build diversity into the system design is an interesting question. Akashi [2], for example, suggests that the *law of diminishing return* plays a central role in the genetic diversity in biological systems.

C. Adaptability

Lastly in this section, because systems that demonstrate an adaptive capacity can generate novel ways of operating or novel systemic associations, they can persist in, or recover from, crises [35]. One of the adaptation mechanisms of biological systems is of course evolution through gene mutations. These mutations could be random, and the variations that fit the current environment most have better chances to survive. This way, species adapt themselves according to the environmental changes. Example of adaptability can be found in warm and cold-bloodied species, who hibernate and aestivate, respectively, to cope with changes in temperature. Another interesting case is that of the hermit crab who must use shells from other animals (e.g., snail shells) for protection against predation and drying out. As an example of engineering system resilience, IBM proposed the concept of Autonomic Computing for IT systems in 2003 [31]. This architecture is based on the so-called Monitor-Analyze-Plan-Execute cycles. More sophisticated than a simple feedback system, it senses the situational changes and reacts automatically to handle the situations, hence, adaptive.

In contrast to redundancy and diversity being mostly concerned with the phases in the resilience cycle that comes prior to a shock, adaptability is at every phase of the resilience cycle, from the design, operation, detection and response to shock, to the recovery. You can build a feedback mechanism in the design so the system can adapt itself gradually as the threat model changes over time, and once the shock occurs, the rest is still about the system adapting while recovering.

While studying the resilience cycle and mapping the strategies onto its different phases, however, we came across an interesting idea of a completely new strategy for resilience.

IV. Stability, Longevity and Severity

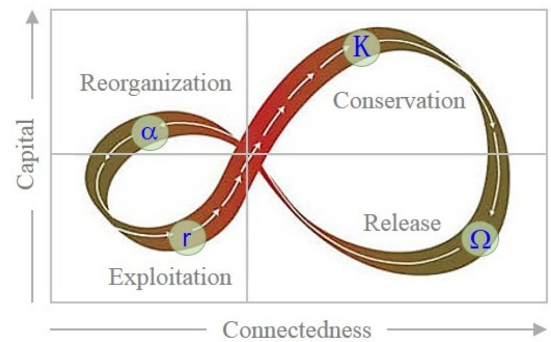
In his insightful book entitled *The Great Stagnation* [16], Tyler Cowen lamented how the US economy enjoyed what he figuratively termed as "low-hanging fruits". One example is the once abundant fertile American land which populations, from the early European settlers and through the ages, enjoyed toiling and reaping – this land was plentiful and free up through the end of the 19th century. Another is the technological breakthroughs and innovations that were streaming from 1880 to 1940, but plateaued around the mid-20th century. The structures that were built to produce and provide what the world enjoyed in their rich returns and significant changes diminished in value. Cowen attributes this stagnation to our current discoveries and innovations being geared towards private, more than public, goods. We may even insert here that this standard has indeed become rigid and tightly knit in our social norms. We further believe that as the world continues in this status quo of relying on low-hanging fruits, whose returns have diminished, there is the need to get off this road that will lead to a societal collapse. This can be one illustration of how a system when allowed to progress in rigidity would eventually collapse. This dynamic has been observed to occur in various sorts of systems and has been put into perspective by a well-known framework commonly cited in the resilience literature, namely, Holling's adaptive cycle.

As he took careful and accurate investigation of the ecology of forests, C.S. Holling observed that healthy forests have an adaptive cycle of growth, collapse, regeneration and growth once again [24][25]. He embedded this observation in the framework shown in Fig. 3. The cycle consists of a slow but gradually growing phase of *exploitation* (r) to *conservation* (K), often referred to as the foreloop of the cycle. The one dubbed as the backloop consists of the transition phase of a quick *release* (Ω) to *reorganization* (α). The foreloop is a slow process characterized by the exploitation and accumulation of the available capital (or potential resources). What is also accumulating, however, is a rigid complexity – not only are the components of the system (e.g., species of the ecosystem) becoming more numerous, their connectedness becomes even tighter and their self-regulation more finely tuned [27] until the system converges to a state that makes itself less adaptive in the presence of a shock. The growth just cannot go on indefinitely and comes a point that the complexity can no longer be sustained and the system collapses. The backloop starts with the sudden release of the complexity, characterized by significant decrease in capital and loss of connections among parts. When this happens, however, the system begins to open itself up to novel forms, functionalities, and systemic associations. Since the foreloop is much longer than the backloop, it is the normal and stable situation, which is preferred over the other much dramatic backloop, which in many cases, comes with significant pain.

Our resilience cycle, which we described in section II, runs in parallel with Holling's adaptive cycle. From our point of view, a system is resilient as long as this cycle continues, and if the system fails to transition to reorganization (α) from release (Ω), the cycle is broken and the system fails to survive. In section III, we discussed the strategies that can decrease the probability of this fatal breakdown.

Fig. 3. Holling's Adaptive Cycle

Apart from keeping the cycle intact, however, we further argue for prolonging the foreloop. Our view is that resilience



should also involve prolonging this desired state of stability while increasing the system's capacity to withstand the damage that a large shock can bring, thereby lessening both the severity of the collapse and the pain that comes with it. This can be achieved by regulating the build-up that Holling aptly put as a disaster in the wings just waiting to transpire.

One strategy is to deliberately inject or induce regularly small controlled (i.e., timely and of the appropriate amount) shocks into the system while the build-up of complexity and rigidity among its components and their functions and connections are on-going. This is a way of regulating the system processes, un-optimizing it in a way, for creative novelty to emerge. In relation to Holling's adaptive cycle, this would mean extending the K-phase by actually regularly disrupting the tightening of interconnections and accumulation of rigidities among parts, and test for novel combinations that may eventually lead to increased system effectiveness.

This kind of strategy is being employed by well-known large datacenters like Amazon, Google and Netflix. Amazon created the original *GameDay* and Google runs an equivalent of it [1]. GameDay is a program specially designed to increase the resilience of an engineering system by intentionally inflicting it semi-regularly with major failures to allow flaws, irregularities and subtle dependencies to surface. A key element of the strategy is to discover the latent defects or bugs by testing some less-exercised system connections (e.g., groups that do not work together in normal situations, a powered-off major datacenter, communication black-out among teams for days, etc.) [1]. In the same spirit of inducing failure at regular time intervals, perhaps more frequent than that of GameDay, Netflix implements a multi-level failure induction mode, called the *Simian Army* [30][48], in the system's live environment. The Simian Army consists of the *Chaos Monkey* that causes failure of virtual instances (e.g., through disk failure or inaccessible network partition), *Chaos Gorilla* that causes an entire availability zone (or datacenter) to fail, and the *Chaos Kong* that causes multiple region-wide datacenters to fail. And there is one more, whose significance cannot be undermined, called the *Latency Monkey* that is invoked to find sick or partially healthy instances but are still working. This agent injects artificial delays to simulate service degradation or node or service downtime without actually shutting down instances in, or services of, the system [48].

The motivating principle behind adopting such a strategy is to let systems embrace the inevitable failure and learn how to deal with it swiftly once it happens. It is more efficient and effective to create situations that can force latent problems to surface than design the system to not fail, which, paradoxically, only makes it less resilient. This strategy will certainly cause panic and discomfort, to say the least, but will last for a relatively shorter time than expected. Interestingly, Netflix's goal of deploying the Simian Army is to make the injected failures *nonevents*, i.e., they happen frequently and in the background, so that when the real failures actually happen, they will simply blend into the situation as mundane [48].

Nature is not also void of this kind of strategy. In ecology, natural fire occurrence is an essential part of the forest ecosystem since it replenishes soil nutrients, allows new plant species to grow, and reduce pathogens and infestations, among others. In evolution, although deleterious mutation is assumed to inject harm and impede adaptive evolution, there are studies that argue for its potential as stepping stone in the evolution of complex new functions (refer to [15] for notable citations).

V. Concluding Remarks

In our attempt to come up with a language that will contextualize resilience, considering its broad scope, we detailed in this paper our proposed taxonomy for general resilience in relation to the general resilience strategies. Furthermore, we also discussed a new strategy for prolonging the stability phase in the light of the inevitable resilience cycle, which is to introduce controlled shocks to regulate its complexity and rigidity. As for the next step, we aim to build mathematical models that can validate the qualitative discussions we put forward in this work.

VI. References

[1] ACM, "Resilience Engineering: learning to embrace failure – A discussion with Jesse Robbins, Kripa Krishnan, John Allspaw, and Tom Limoncelli," *Queue*, vol. 10, no. 9, article 20, pp. 20-28, Sept 2012. Available: http://doi.acm.org/10.1145/2367376.2371297.

[2] H. Akashi, N. Osada, and T. Ohta, "Weak selection and protein evolution," *Genetics*, vol. 192, pp. 15-31, 2012.

[3] ASIS Commission on Standards and Guidelines, *Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use Standard*, ASIS, Nov. 2009.

[4] T. Baba, T. Ara, M. Hasegawa, Y. Takai, Y. Okumura, M. Baba, K.A. Datsenko, M. Tomita, B.L. Wanner, and H. Mori, "Construction of Escherichia coli K-12 in-frame, single-gene knockout mutants: the Keio collection," *Molecular Systems Biology*, vol. 10, Feb 2006.

[5] P. Bak, *How Nature Works: The Science of Self-Organised Criticality*. New York, NY: Copernicus, 1996.

[6] P. Bak, C. Tang, and K. Wiesenfeld, "Self-organized criticality: an explanation of the 1/ f noise," *Physical Review Letters*, vol. 59, pp. 381–384, Jul 1987.

[7] A. Barabasi and E. Bonabeau, "Scale-free networks," *Scientific American*, vol. 288, pp. 50–59, 2003.

[8] P. Brennan, "Lessons learned from the Japan earthquake," *Disaster Recovery Journal*, Summer 2011.

[9] L. Briguglio, G. Cordina, N. Farrugia, and S. Vella, "Economic vulnerability and resilience – concepts and measurements," United Nations University – World Institute for Development Economics Research, May 2008. Available: http://www.wider.unu.edu/publications/working-papers/research-papers/2008/en_GB/rp2008-55/

[10] T. Brudermann and Y. Yamagata, "Towards studying collective dynamics of electricity sharing systems", *Proc. 6th International Conference on Applied Energy*, to appear.

[11] M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, T.D. O'Rourke, A.M. Reinhorn, M. Shinozuka, K. Tierney, W.A. Wallace, and D. von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733-752, Nov 2003.

[12] S.R. Carpenter, K.J. Arrow, S. Barrett, R. Biggs, W.A. Brock, A. Crepin, G. Engstrom, C. Folke, T.P. Hughes, N. Kautsky, C. Li, G. McCarney, K. Meng, K. Maler, S. Polasky, M. Scheffer, J. Shogren, T. Sterner, J.R. Vincent, B. Walker, A. Xepapadeas, and A. de Zeeuw, "General resilience to cope with extreme events," *Sustainability*, vol. 4, pp. 3248-3259, 2012.

[13] S.R. Carpenter, C. Folke, M. Scheffer, and F. Westley, "Resilience: accounting for the noncomputable," *Ecology and Society*, vol. 14, no. 1, article 13, 2009.

[14] J.L. Casti, *X-Events: The Collapse of Everything*. USA: HarperCollins, 2012.

[15] A.W. Covert, R.E. Lenski, C.O. Wilke, and C. Ofria, "Experiments on the role of deleterious mutations as stepping stones in adaptive evolution," *Proceedings of the National Academy of Sciences of the United States of America*, 2013. Available: http://www.pnas.org/content/early/2013/08/01/1313424110.full.pdf

[16] T. Cowen, *The Great Stagnation – How America Ate All the Low-Hanging Fruit of Modern History, Got Sick, and Will (Eventually) Feel Better*. New York: Penguin Group, June 2011.

[17] F. Dalerum, E.Z. Cameron, K. Kunkel, and M.J. Somers, "Interactive effects of species richness and species traits on functional diversity and redundancy," *Theoretical Ecology*, vol. 5, no. 1, pp. 129-139, 2012.

[18] A.S. Downing, E.H. van Nes, W.M. Moaij, and M. Scheffer, "The resilience and resistance of an ecosystem to a collapse of diversity," *PLoS ONE*, vol. 7, no. 9, Sept 2012.

[19] T.B. Fowler, "In depth – finance theory and heavy tails," *Sigma*, vol. 10, no. 1, pp. 44-50, Sept 2010.

[20] T.B. Fowler and M.J. Fischer (eds), "Rare events – can we model the unforeseen?" *Sigma*, vol. 10, no. 1, Sept 2010.

[21] J. Gray, "Towards a more resilient system?" 36 Seattle U. L. Rev. 799, 2013. Available: http://digitalcommons.law.seattleu.edu/sulr/vol36/iss2/15/

[22] L.H. Gunderson, "Ecological Resilience – in theory and application," *Annual Review of Ecology and Systematics*, vol. 31, pp. 425-439, 2000

[23] L.H. Gunderson and C.S. Holling, *Panarchy: Understanding Transformations in Human and Natural Systems*. Island Press, 2002.

[24] C.S. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology and Systematics*, vol. 4, pp. 1-23, 1973.

[25] C.S. Holling, "Understanding the complexity of economic, ecological, and social systems," *Ecosystems*, vol. 4, pp. 390-405, 2001.

[26] E. Hollnagel, D.D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. UK: Aldershot, February 2006

[27] T. Homer-Dixon, "Our panarchic future," *World Watch Magazine*, vol. 22, no. 2, March/April 2009.

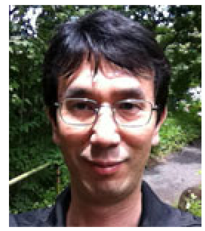
[28] J. Horton, A. Kashdan, K. Nothstine, "Strategies to bolster economic resilience – country leadership in action," National Association of Countries, November 2013. Available: http://www.naco.org/newsroom/pubs/Documents/Strategies%20to%20Bolster%20Economic%20Resilience.pdf

[29] ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, 2013.
[30] Y. Izrailevsky and A. Tseitlin, “The Netflix Simian Army,” *The Netflix Tech Blog*. Available: http://techblog.netflix.com/2011/07/netflix-simian-army.html
[31] J.O. Kephart and D.M. Chess, “The vision of autonomic computing,” *Computer*, vol. 36, no. 1, pp. 41-50, 2003.
[32] J. Kitano, D.I. Bolnick, D.A. Beauchamp, M.M. Mazur, S. Mori, T. Nakano, and C.L. Peichel, “Reverse evolution of armore plates in the three spine stickleback,” *Current Biology*, vol. 18, no. 10, pp. 769-774, May 2008.
[33] R. Lande, “Statistics and partitioning of species diversity, and similarity among multiple communities,” *Oikos*, vol. 76, no. 1, pp. 5-13, 1996.
[34] T.G. Lewis, *Bak’s Sand Pile: Strategies for a Catastrophic World*. Williams, CA: Agile, March 2011.
[35] P. Martin-Breen and J.M. Anderies, “Resilience: a literature review,” The Rockefeller Foundation, September 18, 2011. Available: http://www.rockefellerfoundation.org/blog/resilience-literature-review
[36] H. Maruyama and K. Minami, “Towards Systems Resilience,” *Innovation and Supply Chain Management*, vol. 7, no. 3, 2013.
[37] A.S. Masten, “Ordinary Magic: resilience processes in development,” *American Psychologist*, vol. 56, pp. 227-238, 2001.
[38] A.S. Masten and J. Obradovic, “Disaster preparation and recovery: lessons from research on resilience in human development,” *Ecology and Society*, vol. 13, no. 1, article 9, 2008.
[39] S. Moskovitz, “Longitudinal follow-up of child survivors of the Holocaust,” *Journal of the American Academy of Child Psychiatry*, vol. 24, no. 4, 1985.
[40] D.A. Patterson, G. Gibson, and R.H. Katz, “A case of redundant arrays of inexpensive disks (RAID),” in *Proc. 1988 ACM SIGMOID International Conference on Management of Data*, pp. 109-116, 1988.
[41] A. Purvis and A. Hector, “Getting the measure of biodiversity,” *Nature*, vol. 405, pp. 212-219, May 2000.
[42] A. Ride and D. Bretherton, *Community Resilience in Natural Disasters*. New York, NY: Palgrave Macmillan, 2011.
[43] K.R. Ronan and D.M. Johnston, *Promoting Community Resilience in Disasters*. New York, NY: Springer, 2010.
[44] D. Schleuter, M. Daufresne, F. Massol, and C. Argillier, “A user’s guide to functional diversity,” *Ecological Monographs*, vol. 80, no. 3, pp. 469-484, 2010
[45] J.F. Shortle and C. Chen, “What can lead to a wide-scale blackout,” *Sigma*, vol. 10, no. 1, pp. 44-50, Sept 2010.
[46] J.A. Tainter, *The Collapse of Complex Societies*. Cambridge, UK: Cambridge University Press, 1988.
[47] N.N. Taleb, *The Black Swan – The Impact of the Highly Improbable*. US: Random House, 2007.
[48] A. Tseitlin, “The Antifragile Organization – embracing failure to improve resilience and maximize availability,” *Communications of the ACM*, vol. 56, no. 8, pp. 40-44, Aug 2013.
[49] L. Xu and D. Marinova, “Resilience thinking: a bibliometric analysis of socio-ecological research,” *Scientometrics*, vol. 96, pp. 911-927, 2013.
[50] B.D. Youn, C. Hu, P. Wang, “Resilience-driven system design of complex engineered systems,” *Journal of Mechanical Design*, vol. 133, October 2011.
[51] A. Zolli and A.M. Healy, *Resilience: Why Things Bounce Back?* New York, NY: Free Press, 2012.

VII. Biographies

Hiroshi Maruyama was born in Yokohama, Japan in 1958. He graduated from The Graduate School of Science and Engineering, Tokyo Institute of Technology in 1983. He joined IBM Research, Tokyo Research Laboratory and worked on various computer science fields such as logic programming, natural language processing, machine translation, hand-writing recognition, XML, Web services, and security. From 2006 to 2009, he served as the director of IBM Tokyo Research Laboratory. In 2011, he joined The Institute of Statistical Mathematics where he is engaged in researches on services science and systems resilience.

Roberto Legaspi (M’2011, F’4) was born in Manila, Philippines. He obtained his PhD degree from the Graduate School of Information Science and Technology of Osaka University. He is currently a research associate professor at the Research Organization of Information and Systems, Transdisciplinary Research Integration Center and is working within the auspices of The Institute of Statistical Mathematics. For more than a decade, he has been addressing compelling issues in the area of human behavior computing for human-centric intelligent system interactions. His current research involves looking into various system resilience theories, frameworks and applications through the lens of behavior computing.



Kazuhiro Minami is a research associate professor at The Institute of Statistical Mathematics in Japan. He has been working on security and privacy in pervasive computing particularly focusing on secure information sharing among mutually untrusted parties. He is currently working on new software engineering disciplines for developing resilient ICT systems, which could recover from disastrous situations in a flexible and graceful way. After finishing a Ph.D degree, he spent several years as a lecturer and a postdoctoral researcher at University of Illinois, and then took a position of an associate professor at National Institute of Informatics until March 2012.

Yoshiki Yamagata graduated from the University of Tokyo (PhD in System Science). Since 1991, he works at the National Institute for Environmental Studies (NIES, Tsukuba). Currently, he is studying about the climate risk management as Principal Researcher of Center for Global Environmental Research (CGER). He is also affiliated with IIASA (Vienna) and Institute of Statistical Mathematics (ISM, Tokyo). His recent research topics include: Land use scenarios, resilient urban planning and Spatial network analysis. He has lecture series at the University of Tokyo, University of Tsukuba and Hokkaido University. Internationally, he has contributed as Lead Author of IPCC, Steering Committee of “Global Carbon Project” and Editor of “Applied Energy”, etc.