Towards Systems Resilience

Hiroshi Maruyama
Trans-disciplinary Research Integration Center
The Research Organization of Information and Systems
Tokyo, Japan
hm2@ism.ac.jp

***Abstract*—Some systems are *resilient* – they recover from unanticipated large scale perturbations and continue to exist – while others are not. We started a new project called "Systems Resilience" that aims to study underlying principles of resilience. We study a wide variety of domains, such as biology, ecology, economics, engineering, sociology, and business management, and extract common characteristics that differentiate resilient systems from non-resilient ones. We are building a mathematical model to represent these characteristics and to quantify resilience.**

***Keywords*-resilience; extreme events; redundancy; diversity; adaptability**

I. Introduction

After the 3.11 earthquake there has been significant increase on the discussions on events that are both rare and having significant impacts, sometimes called *X-Events*[1]. These "surprising" events occur as an outside of the anticipated envelope (e.g., Tsunami of 14m high vs the anticipated max of 5.7m), or something completely unheard of (e.g., Tokyo subway gas attack in 1995). "X-Events" are inevitable. They do happen, and our systems may fail. It is not possible, theoretically or practically, to protect our systems for all X-Events. When the system fails, we have to recover from the damage as quickly and as inexpensively as possible. This process may not be exactly a "recovery" because it may or may not restore the system into the original configuration; rather, the system can be in a completely new configuration that is also acceptable, or even desirable, to the stakeholders. The ability to make a system to withstand large perturbations and enable generalized recovery once the system fails is, in our definition, "resilience."

To shed scientific lights to the concept of resilience, we started a multi-year, multi-disciplinary project called "Systems Resilience"[1] in April 2012, within The Trans-Disciplinary Research Integration Center in The Research Organization of Information and Systems, a national research organization under the Japanese Ministry of Education, Culture, Sports, Science and Technology. This paper overviews the project and its current status. We first give our basic assumptions and project goals. Our working hypothesis about resilience strategies are covered in Section 3. In Section 4, we briefly touch on the mathematical model we are building for explaining these strategies, followed by the future directions.

[1]See http:http://systemsresilience.org/index-e.html for the details.

II. Project Goals

Resilience is observed in many different systems; human minds exhibit resilience after suffering real hardship, ecosystems such as rain forests and the Antarctic ocean are known to recover after perturbations, biological systems such as human body can recover from injuries, the global communication systems have survived many technological faults, natural disasters, policy changes, etc., many cities demonstrated that they could withstand large historical events such as pandemics, wars, and geopolitical changes, and so on.

Our basic assumption is that there must be a common set of strategies that make these systems resilient, regardless their own domain, be it a biological, ecological, economical, organizational, or engineering system.

Provided that this assumption holds, our goal is to investigate these common strategies and organize them into an organized body of knowledge (BoK). This "Resilience BoK" will guide us when we design and operate a (social, engineering, or some other) system so that we can make better, scientifically-accountable decisions to make it more resilient. To do this, the BoK will catalogue various resilience strategies and describe when and how these strategies should be applied.

This goal is not easy to achieve. Our approach is to take the following three steps. First, we collect experiences of resilience (and also non-resilience) in many different fields as many as possible, and extract common strategies among them. Second, we build a mathematical model to explain why these strategies work and when. If the model can provide reasonable explanations to the past events, we apply the model to open problems in different fields to verify it.

III. Working Hypothesis

We studied various fields and came to a temporary hypothesis that we can categorize resilience strategies into three categories: *redundancy*, *diversity*, and *adaptability*.

A. Strategy 1: Redundancy

Redundancy is a frequently-used resilience strategy seen in many domains.

Biological systems is known to have a large redundancy. For example, E. Coli has approximately 4,300 genes, each of which has its unique function, but almost 4,000 of them are known to be redundant – that is, knocking out one of them will not hamper its ability to reproduce [6].

Three-spine stickleback is fresh-water fish that had lost their armor plates when they migrated to fresh water from sea water about 10,000 years ago. A sample caught in Lake Washington in 1957 had no armor plates but more recent samples have armor plates. One theory to explain this change is that they regained armor plates because of the predation pressure by trouts whose population had increased during this period due to the increase of the water transparency in the lake. The genotype of the armor plates was dormant (and thus, redundant) during the peaceful years but became active when the necessity arose[2].

In engineering systems, it is a common strategy to have back-up systems to make systems more reliable. For example, mission-critical storage systems use RAID (Redundant Arrays of Inexpensive Disks) so that the system can continue function even though one or more disks fail [5].

Before 3.11, the nuclear power had accounted for about 30% of all the electricity consumption in Japan. Within 14 months after the earthquake, every one of Japan's 50 nuclear power stations went into maintenance cycles and remained non-operational until a few of them restarted a few months later. Although Japan has lost almost a third of its electric generation capacity, Japan has never experienced major blackout during this period. This can be attributed to the centralized and monopolized system of Japanese electric industry. One of their top priorities resides in the stable supply of electricity, and for that purpose Japanese electricity systems have had a huge excessive capacity.

The auto industry was also affected by the earthquake because their extremely complex supply chain depends on a large number of suppliers located in the Tohoku area. Despite the unprecedented scale of damage they suffered, every major auto company in Japan survived the crisis. One of the reasons of their survival was their monetary reserve that could compensate the temporary loss of the revenue. Electricity and money can be considered to be universal resource, and having extra universal resource in reserve is a good strategy for preparing unseen threats.

When the United States was attacked by the terrorists on September 11th, 2001, the police departments, the fire departments, and the secret service had difficulty in communication and coordination due to the lack of interoperability between their communication equipment. Interoperability enables one component to function as a back-up of another component. Thus, interoperability is a form of redundancy in this context.

B. Strategy 2: Diversity

Diversity is the second category of the resilience strategies.

Diversity plays a central role in the survival of biological systems. The first life on the earth appeared about 4 billion years ago. Since then, there have been a number of large crisis that endangered the survival of life. For example, the PermianTriassic extinction event that occured about 251 million years ago caused up to 96% of marine species to become extinct. One of the reasons that the biological systems as a whole survived is because of diversity – some species had better capability to deal with the changing environment.

Diversity is also a common strategy in mission-critical engineering systems. The Boeing 777 is the first commercial airliner whose control systems is fly-by-wire, i.e., the flight is controlled electric signals rather than hydraulic systems. These signals are controlled by a redundant system consisting of three computers. These three computers are based on different hardware and software developed by independent vendors. If these three computers share the same design, a design flaw would make all the computers fail at the same time. By having diversity in the designs, Boeing 777 can withstand a computer failure caused by a design flaw of a single computer.

In the domain of forest management, it is a common wisdom not to extinguish small forest fires and let the patch of the forest rejuvenate. Otherwise, every part of the forest gets older and dryer, and the risk of a large-scale forest fire would much increase. The diversity of the tree ages in the forest is the key to keep the forest resilient.

In investment management, the diversification of the stocks and bonds that are to be invested is a common practice. This is not the optimum strategy if the goal is to maximize the expected returns. To invest all the money on the stock with the highest expected return is the optimal solution if that is the goal. It is also a risky strategy because the investor loses all the money if the company bankrupts. By diversifying the investments, the investor can significantly reduce the risk of catastrophic loss in exchange for a slightly lower expected return.

C. Strategy 3: Adaptability

The third resilience strategy is adaptability, which is defined as a relative speed of the systems capability to adapt against the environmental changes.

Biological systems are known to be very adaptive. One of the adaptability mechanisms of life is *evolution*. When a life reproduces, there are mutations on the genes. 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 environment change. This is a slow process whose speed is determined by the generation cycle of the species.

A quicker adaptation is realized by *feedback* in both biological and engineering systems. Our body temperature is maintained by sensing the situations and secreting hormones. Air conditioning systems monitor the inside and outside temperatures and control their operations.

In IT systems, IBM proposed the concept of Autonomic Computing [3] in 2003. This architecture is based on so-called the MAPE (Monitor - Analyze - Plan - Execute) cycles. It is more sophisticated than a simple feedback system, but the fundamental strategy is to make the system more adaptable – it senses the changes and react automatically to handle the situations. Thus, it is another example of the adaptability strategy.

D. Active Resilience

So far we discussed three resilience strategies, namely, *redundancy*, *diversity*, and *adaptability*. These strategies do not require human intervention and appear in any resilient systems. We call these *passive resilience*.

Some systems such as human minds, financial systems, organizations, and social systems have human intelligence in their decision loop. We call this type of resilience strategy *active resilience*. Active resilience introduces another set of dimensions to our catalogue of resilience strategies.

If we can *anticipate* a large scale event, we can prepare for it. WHO defines six phrases of pandemic alert. When avian flue H5N1 pandemic was a major threat in 2009, the global society at large responded based on the phase 4-6 declarations by WHO. Japan Meteorological Agency issues warnings on large scale natural events such as typhoons, volcanic activities, and tsunami. Accurate anticipation of such events is extremely hard and generally requires a lot of intelligence and computation.

Modeling is another possibility. When a disaster occurs, collecting information, analyzing it, building models, and making plans based on these models are other areas that human intelligence can play key roles. SPEEDI (System for Prediction of Environmental Emergency Dose Information) is designed for this purpose. It collects information of major nuclear incidents and issues predictions based on there models (unfortunately this system was not effectively used when Fukushima nuclear power plant exploded).

Business Continuity Planning (BCP) is now a standard practice for enterprises. ISO 22320 defines requirements on the management processes for emergency. It stresses the importance of empowering the employees in the bottom of the hierarchy who are dealing with the situation. They need to make tough decisions. They need to improvise. The management process should be designed so that their creativity is encouraged in emergency.

Human intelligence generally enhances the system's resilience. However, active resilience may introduce a new source of error unique to human intelligence – *cognitive errors*. People may overestimate the threat of certain types, such as terrorism, and may overreact.

How to recover from the shock usually requires *consensus building* among stake holders. A disaster may present an opportunity to scrap and re-build the system from scratch. But first we have to identify the stakeholders and ask for their consensus. This is also a unique aspect for active resilience.

E. Tradeoff

In general there are tradeoffs among the strategies we discussed. The available resource (e.g., budget) is limited. Should we invest our resource on redundancy, diversity, adaptability, or active resilience? Investing too much on redundancy by having n-way backup systems may delay the system update cycle and thus may hamper the adaptability for the business environment. What combination of resilience strategies is optimum under a given condition is one of the questions that we would like to answer in our project.

IV. The Model

The second step of our research is to build a mathematical model to study why these strategies work and in what conditions. We assume that a system status can be described in a finite expression. Without loss of generality, a system status can be represented as a bit string of length n. At any given time, the system takes one of the 2^n possible configurations.

A system operates in an environment. A system configuration may be *fit* against the environment. The fitness could be represented by a cost function on the configuration. For simplicity, let us assume here that the cost function can be represented as a set C of all fit configurations. A system configuration s is said to be *fit* iff $s \in C$.

Suppose that there is a shock of type D (say, earthquake of magnitude 7) and the environment changes from C to C'. If the current system configuration s becomes unfit, that is, $s \notin C'$, the system needs to adapt to the new environment as quickly as possible by flipping some bits in s. One way to model this process is that the system fixes one bit at a time. If the system can fix its configuration for any perturbations of type D within k-steps, we call the system k-resilient.

This is the simplest case of our model. More general definition can be found in [4].

V. Future Steps

Our catalogue of resilience strategies is by no means complete. This is an open-ended quest and we continue to look at more domains and extract insights from them.

Our first mathematical model of resilience is defined and now are are to apply the model to the known strategies and try explain why these strategies work in what situations. Also we expect that the model can give some explanations to unsolved, open-questions in certain areas, such as why the ecosystem in the Antarctic Ocean is stable despite the fact that it is very simple (and less diverse).

Our *Systems Resilience* project is fundamentally transdisciplinary. We cannot achieve our goals without having collaboration with diverse fields, many of which are still beyond our radar scope. We are extending our network. If you are interested in, please contact us.

References

[1] John Casti. *X-Events: The Collapse of Everything*. William Morrow, 2012.

[2] J. Kitano, et al. Reverse evolution of armor plates in the trheespine sticleback. *Current Biology*, 18, 2008.

[3] J. Kephart and D. Chess. The vision of autonomic computing. *IEEE Computer*, 2003.

[4] N. Schwind, et al. Systems resilience: a challenge problem for dynamic constratint-based agent systems. *Proc. of the 12th Int. Conf. on Autonomous Agents and Multianget Systems (AAMAS)*, 1988.

[5] Randy H. Katz Patterson, David; Garth A. Gibson. A case for redundant arrays of inexpensive disks (raid). *SIGMOD*, 1988.

[6] T. Baba, et. al. Construction of escherichia coli k-12 in-frame, single-gene knockout mutants: Keio collection. *Molecular Systems Biology*, 10, 2006.