Task Group Summary 3

How can we enhance the robustness via interconnectivity?

Challenge Summary

In contrast with most human designs, which are prone to failures once their components fail, natural and some human-made but self-organized systems display a high degree of robustness to component failures. Indeed, living systems can carry on their activity despite the many molecular errors at the cellular level and the Internet does not collapse despite the fact that at any moment hundreds of routers are not functional. Many living systems, like bacteria, have been shown to be able to withstand the removal of several key enzymes. It is increasingly believed that the robustness of these systems is rooted in their networked nature. Early attempts to address a network's response to attack and failures indicated that real networks are highly robust to random failures but fragile against attacks. Subsequent work has shown that the interplay between the resources and the demand can lead to cascading failures, uncovering a high degree of fragility of some systems. A good example is offered by the US electrical power grid, whose cascading East Coast breakdown was initiated by local failures. In general, a series of recent studies suggest that networked systems are not only robust but also suffer from *vulnerability due to interconnectivity,* as local failures can spread and turn global.

Despite the recent fundamental advances, a deep understanding of the origins and mechanism or robustness across many complex systems is lacking. Little is known, for example, of the role of the dynamics (communication protocols, flow processes) on the network, and how the dynamics and the topology influence each other to promote or undermine robustness. Thus the role of the present working group is to explore what factors contribute to a system's robustness. To achieve this goal, the group is asked to choose a system that is of major importance for the research community and explore the origins of robustness in this system. The system of choice could range from manmade systems, like the Internet or other communication networks, to natural systems, like the cell or an organism.

Key Questions

- What are the proper metrics of robustness?
- How does one quantify the relative contributions of network structure and dynamical effects to robustness?
- Are there universal design principles to robust systems?
- Is robustness more than redundancy?
- Designing networks that are robust to both failures and attacks.
- Cascading failures—can they ever be remedied?
- What measures are appropriate to enhance robustness on a given system?

Required Reading

Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex networks. *Nature* 2000;406:378–482.

Motter AE. Cascade control and defense in complex networks. *Phys Rev* L*ett* 2004;93(9):098701. [http://lanl.arxiv.org/PS_cache/condmat/pdf/0401/0401074v2.pdf.}

Barabási A-L, Bonabeau E. Scale-free networks. *Scientific American* 2003:May:50-59.

Suggested Reading

Levin SA, Lubchenco J. Resilience, robustness, and marine ecosystem-based management *Bioscience* 2008;58(1):27-32.

Paul G, Sreenivasan S, Havlin S, Stanley HE. Optimization of network robustness to random breakdowns. *Physica A*2006;370:854-862.

Barkai N, Leibler S. Robustness in simple biochemical networks. *Nature* 1997;387(6636):913-917.

Due to the popularity of this topic, two groups explored this subject. Please be sure to review the second write-up.

TASK GROUP MEMBERS – GROUP B

- Kirstie Bellman, The Aerospace Corporation
- Jennifer Couch, National Institutes of Health
- Raissa D’Souza, University of California, Davis
- Tony H. Grubesic, Indiana University
- Stephen J. Kron, The University of Chicago
- Luis Rocha, Indiana University
- Caterina Scoglio, Kansas State University
- Alejandra C. Ventura, University of Michigan
- Stuart Fox, New York University

TASK GROUP SUMMARY – GROUP B

By Stuart Fox, Graduate Science Writing Student, N*ew York University*

Fragility is an inherent component of all systems. But unlike a simple system, in which fragility is equally distributed, complex systems present an uneven landscape of strength and weakness. As a result, robustness, the ability of a system to limit, within some specified range, the magnitude of change in performance with respect to perturbations, can only be understood, enhanced, or engineered with the proper intellectual framework. Researchers at the 2008 National Academies Keck *Futures Initiative* Conference on Complex Systems were unable to develop a complete version of that intellectual system; nonetheless, the Task Group (3B) successfully identified the key questions that the intellectual framework would need to answer, and began the process of constructing that framework.

The first step in understanding robustness is acknowledging that robustness is context dependent. This quickly became apparent as the group attempted to answer its original question, which focused on interconnectivity and robustness. In some cases, like a gene regulatory network, more connections mean more robustness. But it is not hard to imagine a reverse scenario, like increased plane travel helping spread a deadly pandemic, where interconnectivity decreases the robustness of a system.

It turns out robustness does not result from finite set of qualities, the application of which could steel any system against failure, but instead depends on the system in question, the goals of the system and the perturbations that system faces. Different strategies will work for some systems and not others. Robustness may mean preservation or adaptation depending on the system, and there is always a cost.

The cost may come in the form of money, metabolic energy, loss of robustness against a different set of perturbations, and many more forms. In fact, the costs of robustness are as numerous as the strategies for creating and enhancing it. The costs of robustness can never be eliminated, only shunted from one area of the system to another.

The very dependence of robustness on context naturally suggests a vague outline of the intellectual framework needed for the understanding of robustness in specific examples, and for the engineering of robustness in man-made complex systems. That framework, at least insofar as the group was able to divine, requires asking four key questions: What is the goal of the system? What are the perturbations? What strategies preserve the goal of the system in the face of those specific perturbations? And what is the cost of each strategy?

To test the elegance of those questions, the group used that preliminary framework to analyze four model systems (see Table 1). Looking at each system, whether natural or man-made, the group found that the robustness strategies lend themselves to grouping far more naturally than the goals of the systems, the perturbations, or the costs. This early result hints that while perturbations and costs vary as widely as complex systems themselves, there may be a finite set of robustness strategies applicable in different situations (see Table 2).

The first, and simplest, systems the group looked at were the proteins RNAse A and green fluorescent protein (GFP). RNAse A is an enzyme that cuts up RNA molecules in liver cells and serves as the standard biochemical model for protein studies. It gained that model status when Armour & Co., the company that makes Armour hotdogs, purified 10 kilograms of the material and distributed the enzyme for free to research institutions. GFP is a luminescent protein found in jellyfish that is widely used as a marker for biological processes in experiments.

Both proteins are far more robust than other similar proteins in the face of denaturing as a result of heat or pH, being cut up, and to the replacement of component amino acids with other amino acids. When the proteins are denatured and the perturbations of heat or pH are removed, or the cut up parts of the proteins are put together and heated, the proteins spontaneously reform. If they are improperly assembled, the proteins still retain some functionality.

That robustness comes at the cost of adaptation. The robustness focuses on maintaining a consistent form, preventing the proteins from undergoing any changes that might enhance the robustness of the protein in the face of other perturbation.

Another biological system the group examined was the nervous system, both central and peripheral. The central nervous system consists of the brain and spinal cord, and controls cognition. The peripheral nervous system connects the brain to the rest of the body, and controls all other functions. The nervous system faces perturbations such as chemical imbalance, change in pH, loss of oxygen, prion disease, stroke, and blunt force trauma, among others. To deal with those problems, the nervous system uses nearly every robustness strategy known to science. For example, a hard skull protects against trauma, an immune system protects against disease, redundancy protects against stroke and single channel failure, flight or fight response avoids or defeats threats to the system.

The cost of that wide spectrum of robustness comes in the form of metabolic energy and design time. The brain takes up most of the energy in the body, and a lot of food is needed to fuel a brain that can think its way around perturbation. As far as design time goes, it took evolution hundreds of millions of years to progress from the simplest nerves to the human brain.

Of the man-made systems that can be analyzed for robustness, the group spent the most time examining the federal highways. The government created the highway system in the 1950s to ensure cross continental military supply lines would not be interrupted by Soviet nuclear attack. As the threat of nuclear war receded, the highway system shifted to primarily providing travel arteries for citizens and companies. In both cases, traffic congestion, blockages and link failures were identified as problems.

Making sure people, products and tanks get where they are going in the face of those problems requires multiple paths to the same destination, increased linkage between the roads of the federal highway system and state and local highways, and geographic distance between hubs to protect against catastrophic, regional problems like hurricanes and nuclear explosions.

Robustness of the highway system has both straightforward and more nuanced costs. The obvious cost is money. Construction and maintenance of the highway system need to be funded. The more subtle cost arises through a concept called Braess' paradox. It turns out that the robustness strategy of adding more roads to decrease congestion actually leads to more traffic in some cases.

While these examples set the group on the right track, many questions remain unanswered. How does one generalize strategies from examples? How best to implement a general robustness strategy with the proper specific detailed information to make it work on the target system? What benefits and costs do different general robustness strategies provide for specific complex systems? Moving forward, the group decided to continue working on this problem, and over the course of time, to finish developing the framework for understanding, leveraging and enhancing the robustness of complex systems.

TABLE 1 Example Systems

System	Perturbation	Strategy	Cost	What Is Preserved
RNAse A, GFP	Temp, pH, cutting into piece	Self-healing, redundancy	Failure to adapt, design time	Enzymatic function, glowing
Central and peripheral nervous system	Temp, chemicals imbalance, tumors, stroke, blow to the head, etc.	Hardening, diversity, avoidance… everything in Table 2	Metabolic energy (vastly disproportionate consumption), design time	Life, cognition, ability to adapt
Federal highway network	Congestion, blockages, link failure	Diversity of paths, spatial separation, provisioning	Construction, maintenance	Transport, origin-destination paths, flow
Gene regulatory network	Mutations, environmental conditions, development stages	Canalization, connectivity, redundancy, multitasking	Constructing additional molecules, design time	Phenotype, multiple viable modes (adaptability)

TABLE 2 General Robustness Strategies

- Redundancy (repetition, substitution, overlap)
- Diversity
- Modularity
- Spatial separation
- Fortification
- Buffering
- Cutting losses
- Canalization
- Avoidance
- Connectivity
- Multiple viable modes
- Feedback
- Smart nodes/smart edges
- Self-healing
- Regeneration
- Balancing control between centralized and decentralized components
- Trusted/collective intelligence for centralized aspects
- Computational reflection (system's awareness and planning of resource allocation)