Robustness of Structures
COST Action TU0601
1st Workshop, February 4-5, 2008, ETH Zurich, Zurich, Switzerland

Risk-based assessment of robustness: what can it do and what can't it do?

Jack W. Baker
Assistant Professor, Civil and Environmental Engineering, Stanford University
Yang & Yamasaki Energy & Environment Building, Mail Code 4020, Stanford, CA 94305, USA
bakerjw@stanford.edu

Abstract

A guiding principle in the design of structures is to maximize the reliability of a structural system (that is, to minimize the probability of failure, or perhaps more generally to minimize the risk associated with potential failures). Robustness has been recognized as a valuable property to incorporate into systems, in support of that principle. A discussion of possible methods for quantifying robustness is presented here, along with an argument as to why risk- and reliability-based methods may be useful for quantifying robustness and for evaluating robustness-related design criteria. The second part of the paper discusses the concept of robustness from the perspective of Normal Accident Theory and the System-Action-Management framework for risk assessment. These concepts both recognize that complex systems have difficult-to-identify feedback loops that may cause failure mechanisms that are difficult to identify *a priori*. Redundant systems are often coupled, so that backups fail in the same event that causes failure of a primary system. Establishment of backups can also increase system complexity and encourage risk-taking by designers or operators. Design of high-rise residential buildings in the seismically-active western United States is used an example to discuss these concepts. While there are methods available to deal with these challenges, quantitative measures of robustness should be treated as only a partial solution if they are computed without recognizing the potential for complex failure sequences.

1 Introduction

Arguably, a guiding principle in the design of structures is to maximize the reliability of a structural system (that is, to minimize the probability of failure, or more generally to minimize the risk associated with potential failures). Within that overarching principle, robustness has been recognized as a valuable property to incorporate into systems.

If we knew the structural system, and its environment, perfectly (in a stochastic sense) we could simply optimize the structure for maximum reliability without regard to properties such as redundancy or robustness. However, experience shows us that often our analytical models are only approximate, they omit factors such as human error, fail to identify cascading failures, or underestimate the probability of occurrence of unusual loads. If our models fail to capture these effects, then it may be valuable to add additional considerations to our design goals in order to provide additional insurance against failures due to these effects. That is why criteria related to robustness are valuable: they are intended to minimize the system's risk by adding requirements that will result in acceptable performance under unanticipated loading.

One approach to adding this robustness is to look for failure mechanisms where a small initial perturbation leads to a cascading failure. This is helpful for two reasons. First, our load model may suggest that the perturbation is unlikely and thus the structure is reliable, but it is good insurance to avoid the possibility of this outcome anyway in case our model is wrong (as one might argue was the case with the Ronan Point collapse). Human error and extraordinary loads are two examples where this robustness approach might lead to a safer structure, even if a formal reliability calculation (which may omit or trivialize these factors) might not suggest that measures are needed. A second benefit of adding robustness requirements is that looking for cascading-failure situations may lead to general design principles (such as tying components together) that can be applied without performing a complete risk assessment. Such principles then have the potential to be codified as robustness guidelines.

Many of these codes specify that structures should be robust in the sense that "the consequences of structural failure should not be disproportional to the effect causing the failure."

2 General robustness assessment methodologies

If one agrees to perform a probability-based assessment of robustness, there are several existing proposals available. Two examples of probability-based assessment approaches are briefly summarized here for illustration. Additional general approaches are summarized elsewhere (Canisius et al. 2007). Approaches specifically focused on preventing progressive collapse have also been summarized elsewhere (Ellingwood 2006).

2.1 Reliability-based assessment

Lind (1995; 1996) proposed a generic measure of system damage tolerance, based on the increase in failure probability resulting from the occurrence of damage. He defined the vulnerability (*V*) of a system as

$$V = \frac{P(r_d, S)}{P(r_0, S)} \tag{1}$$

where r_d is the resistance of the damaged system, r_0 is the resistance of the undamaged system, and S is the prospective loading on the system. $P(\cdot)$ is the probability of failure of the system, as a function of the load and resistance of the system. This vulnerability parameter indicates the loss of system reliability due to damage.

There are several reliability-based measures such as that in equation (1), and they are all useful in that they quantify the increased probability of system failure caused by damage to a component. If a small level of damage significantly increases the probability of system failure, than one could reasonably say that the system has a lack of robustness.

2.2 Risk-based assessment

Baker et al. (2006) proposed another metric for robustness of an engineered system. It is a natural extension of the previous section, in that it attempts to identify problems caused by damage to a system within the context of probabilistic assessment. The extension here is to also incorporate the consequences of damage and failure, so that the calculation becomes risk-based rather than reliability-based. Given that our working definition of robustness is that "the *consequences* of structural failure should not be disproportional to the effect causing the failure," it is desirable to have a measure of consequences included in the calculation.

The approach divides consequences into direct consequences associated with local component damage (that might be considered proportional to the initiating damage) and indirect consequences associated with subsequent system failure (that might be considered disproportional to the initiating damage). An index is formulated by comparing the risk associated with direct and indirect consequences. The index of robustness (I_{Rob}) is defined as

$$I_{Rob} = \frac{R_{Dir}}{R_{Dir} + R_{Ind}} \tag{2}$$

where R_{Dir} *and* R_{Ind} are the direct and indirect risks, respectively. These risks are defined as illustrated in Figure 1. First, an exposure occurs which has the potential of damaging components in the system; this is termed the exposure before damage, or EX_{BD}. If no damage occurs ($\bar{D}$), then the analysis is finished. If damage occurs, a variety of damage states (D) can result. For each of these states, there is a probability that system failure (F) results. Consequences are associated with each of the possible damage and failure scenarios, and are classified as either direct (C_{Dir}) or indirect (C_{Ind}).

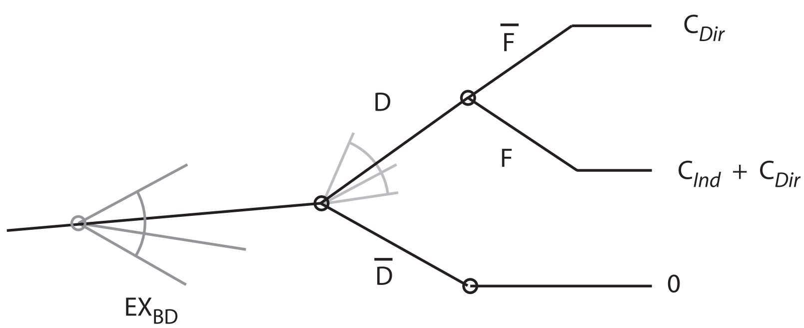

Figure 1: An event tree for robustness quantification (from Baker et al. 2006).

Given that the needed probabilities are available, and that the consequences of each outcome can be assessed, the direct and indirect risks can be computed as

$$R_{Dir} = \int_x \int_y C_{Dir} \, f_{D|EX_{BD}}\left(y \,|\, x\right) f_{EX_{BD}}\left(x\right) dy dx \tag{3}$$

$$R_{Indir} = \int_x \int_y C_{Indir} P\left(F \mid D = y\right) f_{D|EX_{BD}}\left(y \mid x\right) f_{EX_{BD}}\left(x\right) dydx \tag{4}$$

where $f_Z(z)$ is used to denote the probability density function of a random variable *Z*. A Markovian assumption has been made in the above equations (i.e. the probability of failure of a system with a given damage state is assumed to be conditionally independent of the exposure causing the damage). This conditional independence can sometimes be achieved by carefully the damage states so that the damage state carries all information needed to compute probabilities of future failures.

The index given in equation (1) takes values between zero and one, with larger values indicating larger robustness. The motivation for this index is that systems having high risk associated with indirect consequences are more likely to suffer disproportionate damage consequences and thus be less robust. In addition to quantifying the effect of the physical system's design, this approach can potentially account for the effect of inspection, maintenance and repair strategies as well as preparedness for accidental events, because those actions can reduce failure consequences and thus risk.

The framework is most useful if it can be used for decision-making, and Figure 2 below illustrates how this might be done. The additional symbols in that figure as follows. Design actions (a_d) pre-damage decisions such as inspections and monitoring. Response actions (a_r) could include warning systems and repair actions. Response actions are only taken if damage is indicated (*I*). A second exposure, EX_{AD}, is included in this tree to events with potential to cause additional damage. The framework can thus now account for the increased vulnerability of the structure in the future. Post-damage actions depend upon detecting damage (the probability of which is affected by the inspections and monitoring actions which are here assumed to be part of the design decisions). Based on the damage level of the system, and the actions taken as a result of detection, the system has a probability of failure due to post-damage exposures (EX_{AD}).

It is implied that if damage is indicated, then action will be taken either to reduce failure consequences (e.g. by evacuating a structure) or the probability of failure (e.g. through repairs). The probability of damage detection will depend on inspection choices, the type of damage, and the type of exposure causing damage. For example, damage from explosions will likely be detected, while corrosion of an inaccessible component may not be detected.

The basic choice of design action is now also explicitly included at the beginning of the tree. These actions will include design of the physical structure, maintenance to prevent structural degradation, inspection and monitoring for identifying damages, and disaster preparedness actions. These actions, along with the post-damage response actions, will affect the probabilities and consequences associated with the other branches, and so this decision tree can be used as a tool to identify actions which minimize risk and maximize robustness in a system. When alternative systems have varying costs, then these costs should be included in the consequences (and the branch of the tree corresponding to $\bar{D}$ will no longer have zero consequences for some system choices). This representation of a system can be used to design systems that minimize total risk.

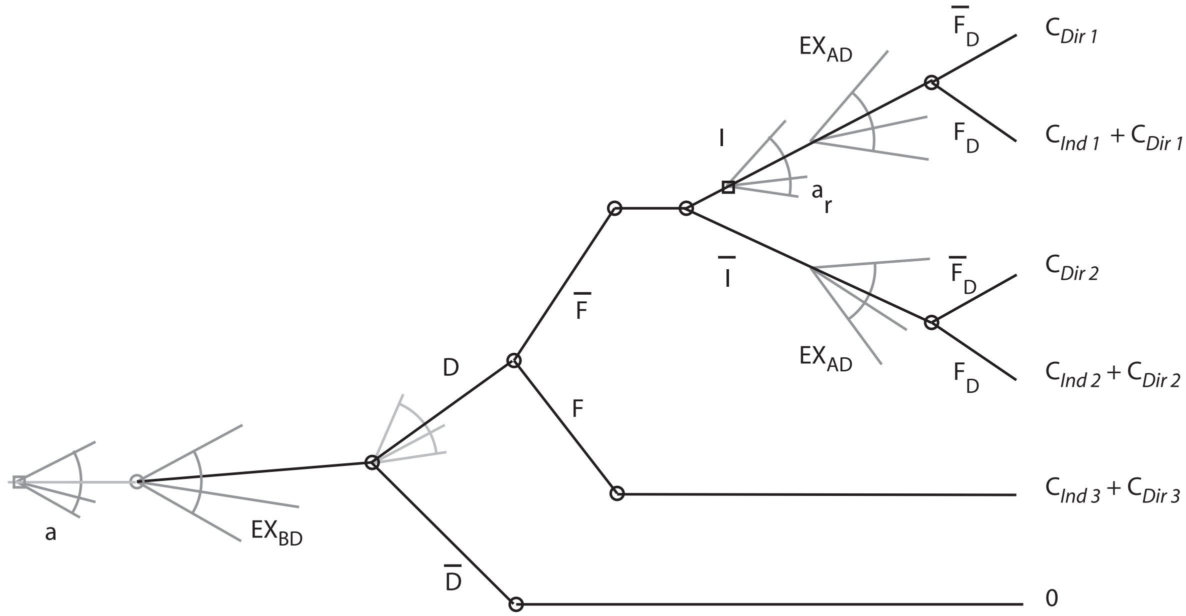

Figure 2: An event tree that incorporates system choice and post-damage exposures (from Baker et al. 2006).

A possibly-negative feature of this risk-based approach relative to the reliability-based assessment above is that it results in an additional challenge for quantifying consequences as well as reliability. On the other hand, most design codes speak of "consequences of failure," which seems to require consideration of both failures and consequences. Perhaps the effort to quantify consequences is feasible for a calibration exercise to establish simplified design guidelines.

Results obtained using this calculation approach (Baker et al. 2006; Schubert and Faber 2007) indicate that properties affecting system reliability, such as number of redundant components or the stochastic properties of the load, also affect this robustness index. Perhaps more interestingly, it is seen that properties such as failure consequences and time to repair a damaged system also affect this measure of robustness.

3 Discussion

While purely analytical quantifications of robustness should prove useful in furthering robustness research and in developing code criteria, it is also useful to consider qualitative concepts when searching for features of robust systems.

3.1 Impacts of redundancy

Redundancy in the sense of static indeterminacy can provide false comfort. Calibration of system performance as a function of this type of redundancy has been preformed for seismic safety (Wen and Song 2003). That work found that, among buildings with comparable lateral strength, reliability under earthquake loading was only moderately improved by using structural configurations with additional redundancy. This is because the capacity of redundant elements is typically highly correlated and because the uncertainty in seismic loading is relatively large compared to the uncertainty in capacity. The findings were focused on seismic loading only, but similar calibration studies could be considered for other loading types.

An interesting application of redundancy concepts is in the recent surge in tall buildings design in seismically active areas. Traditionally, tall buildings in high seismic areas were required to have two lateral force resisting systems (often a shear wall or braced frame in the core of the building, and a moment resisting frame at the perimeter). Because the perimeter moment resisting frame obstructs views and leads to increased story heights, many new buildings are being designed without this secondary redundant frame system. While the removal of the redundant system might decrease the reliability of the building, these designs are incorporating increased capacity in their other load resisting systems, and are being subjected to rigorous peer review standards and are causing new research to be conducted (Moehle and Yang 2007). Whether the increased design scrutiny completely offsets the loss of the perimeter moment frame is unknown, but there certainly seems to be an interaction where consciousness of reduced redundancy leads to greater vigilance in other aspects of the design and construction project.

Rather than focusing on the non-redundant tall buildings, we can reverse the comparison and think about supposedly redundant tall buildings that do not receive the same level of scrutiny. Is the reduced scrutiny because the buildings are more redundant and thus safer? Is it because we have more design experience with these systems and thus need to worry less about unanticipated failure mechanisms? Or is the redundancy providing a false sense of security?

Normal accident theory (Perrow 1984) notes that failures are generally not caused by a single event, but by a sequence of events. Apparently redundant systems can fail because the sequence of events is more tightly coupled than imagined, because the systems are subject to feedback loops, or because there are opportunities for the failures to cascade across the redundant components. In this view, redundancy can cause failures rather than prevent them, it increases system complexity and opaqueness, and encourages risk-taking.

Another concept that may be useful in evaluating redundancy is the System-Action-Management (SAM) framework for evaluating the impact of human behavior on system risk (Murphy and Pate-Cornell 1996). This framework notes that human factors are often the source of failures in complex systems, and that classical risk analysis techniques have difficulty in incorporating these failures quantitatively. The SAM approach advocates incorporating management policies such as incentives and training into the risk analysis, and understanding how they will affect actions of operators who may trigger failures. In the specific case of structural design, management factors will include building code policies, but also pressures due to low fees or tight timelines for design. Complex robustness criteria risk reducing the reliability of structures if they add too much pressure to designers, such that they do not have time to consider detailed design, or they have a sense that the robustness guidelines provide a level of security that can replace basic engineering principles. Given that some robustness descriptions aim to account for the effect of human error, the SAM framework may provide useful guidance when thinking about these issues.

These issues are raised here not to discredit the usefulness of redundancy, or to discourage the development of robustness guidelines, but rather to remind readers that design guidelines have the potential to produce unintended consequences and that any revision to design guidelines should not be evaluated in isolation from the many interacting actions and guidelines that affect system design.

3.2 Redundancy in data networks: a useful comparison?

When searching for robustness criteria to incorporate into building design, it may be useful to understand ways in which robustness has been quantified in other systems. One system in which robustness is a major concern is data networks (either private company networks, or public networks such as the internet). Data networks use three major techniques to establish robustness:

1. Duplicate components. Physical hardware necessary for operation of the network is duplicated, so that backup hardware is available in case the primary hardware fails.
2. Duplicate links/paths. There is more than one route for data to move from point to point, so that if a path is disrupted, alternate paths are available.
3. Duplicate data/content sources. The product (data) is "mirrored," or provided in more than one location. That way, even if a component or path is disrupted and no backup component/path is available, the data is still available from an alternate location.

Comparing these techniques to those used in structures, the first two items seem closely linked to principles that require redundant structural components and alternate load paths. It is noteworthy that complex systems analysis and network analysis are fairly quantitative tools for analyzing data network performance. Can a similar effort be made to quantify alternate load paths in structures?

For the third technique used to build redundant data networks, it is harder to draw an exact parallel with structural design, because if life safety is a concern then the structure must perform whether or not there is a backup facility elsewhere. But in the case of non-collapse system performance, this might be an interesting concept. An interesting example is the design of high-rise towers mentioned earlier. Many of these towers are designed for residential use, rather than commercial use as many previous high-rises have been used for. It has been suggested that residential towers should have higher design criteria than office towers, because people can work elsewhere more easily than they can live elsewhere. Is this a case of redundant office facilities providing robustness? There are sometimes "structural importance" considerations in robustness guidelines, but should there also be "duplicate facility" guidelines? These questions may be worth considering when developing new codified robustness guidelines.

4 Conclusions

Robustness assessment methodologies should preferably be quantitative, in order to facilitate comparison of alternative designs and evaluate design criteria for possible codification. Two concepts for quantifying robustness or redundancy were described, to illustrate how the concept of robustness might be interpreted in the contexts of system reliability and risk management.

Beyond those quantitative measures, however, a word of caution is necessary when attempting to quantify failures in complex or redundant systems. Concepts from Normal Accident Theory, the System-Action-Management (SAM) framework were discussed, to highlight that failures in complex systems often occur due to unexpected interactions and feedback loops. Efforts to create system redundancy can sometimes backfire, because they have caused added complexity that leads to an oversight, or because apparent redundancies lead to risk-taking by designers and operators. If quantitative robustness assessments do not account for these important issues, then decisions regarding robustness should somehow account for these issues through other means.

A brief discussion of redundancies in data networks was also presented, to draw parallels with robustness concepts for structures. Data networks rely on duplicate network components and duplicate paths, which have similarities with redundancies and multiple load paths in structures. Data networks also rely on data mirroring, where the data of value is stored in multiple locations. This concept has similarities with duplicate facilities in structures. It has recently been seen in seismically-active parts of the United States that high-rise residential buildings are being held to higher design standards than high-rise commercial buildings, in large part because people can work elsewhere more easily than they can live elsewhere if the building were to be damaged in an earthquake. Perhaps this points more generally to the possibility for robustness requirements that take into account the availability of duplicate facilities.

Although robustness is a laudable goal and efforts to create redundancy in structures are certainly worthwhile, it is also important to check that any new procedures do not create counterproductive feedback loops, and to consider that the potential for unexpected failures when evaluating a system's safety. More work is needed to quantify this sometimes-abstract ideas, but the effort should pay off in systems having increased reliability.

Acknowledgements

The author thanks Michael Faber, Matthias Schubert, Kazuyoshi Nishijima and Daniel Straub for useful discussions that lead to several of the concepts presented here.

References

Baker, J. W., Schubert, M., and Faber, M. (2006). "On the assessment of robustness." *Structural Safety*(in press).

Canisius, T. D. G., Sorensen, J. D., and Baker, J. W. (2007). "Robustness of Structural Systems – A new focus for the Joint Committee on Structural Safety (JCSS)." *10th International Conference on Application of Statistics and Probability in Civil Engineering (ICASP10)*, Tokyo, Japan, 8.

Ellingwood, B. R. (2006). "Mitigating Risk from Abnormal Loads and Progressive Collapse." *Journal of Performance of Constructed Facilities*, 20(4), 315-323.

Lind, N. C. (1995). "A measure of vulnerability and damage tolerance." *Reliability Engineering & System Safety*, 48(1), 1-6.

Lind, N. C. (1996). "Vulnerability of damage-accumulating systems." *Reliability Engineering & System Safety*, 53(2), 217-219.

Moehle, J., and Yang, T. Y. (2007). "The Tall Buildings Initiative." *Proceedings of the Structrural Engineers Association of California (SEAOC) 2007 Convention*, Lake Tahoe, CA, 10.

Murphy, D. M., and Pate-Cornell, M. E. (1996). "The SAM Framework: Modeling the Effects of Management Factors on Human Behavior in Risk Analysis." *Risk Analysis*, 16(4), 501-515.

Perrow, C. (1984). *Normal accidents : living with high-risk technologies*, Basic Books, New York.

Schubert, M., and Faber, M. H. (2007). "Robustness of Infrastructures Subject to Rare Events." *10th International Conference on Applications of Statistics and Probability in Civil Engineering*, Tokyo, Japa

Wen, Y. K., and Song, S.-H. (2003). "Structural Reliability/Redundancy under Earthquakes." *Journal of Structural Engineering*, 129(1), 56-67.