Protective Systems: Regulation and Grid Stability

Ernie Kee

March 2021

Background (added November 2026). In mid-February 2021, Winter Storm Uri drove electricity demand in Texas far above what could be supplied, as frozen equipment and fuel supplies took generating plants offline. The Electric Reliability Council of Texas (ERCOT), which operates most of the state's grid, ordered rotating outages; millions of Texans were without power for days in freezing weather, and hundreds died. Much of the public criticism focused on the Texas grid's separation from the rest of the country. Ernie Kee wrote this essay a few weeks later. It applies the framework he and Martin Wortman had developed for protective systems in nuclear power—who pays for protection, who benefits, and who bears the harm when protection is absent—to the electric grid, and argues that reliable reserve capacity is a protection regulators must require and ratepayers must fund. The text has been edited for clarity; the argument is unchanged.

Abstract

We examine how protective systems relate to production systems, and the critical role protective systems play in meeting citizens' need for access to energy. We define the scope of protective systems and argue that they exist because regulation requires them; investors would not otherwise adopt them. Investors, beneficiaries, and involuntary stakeholders value protection differently, in both magnitude and direction, and that difference creates a tension, especially between regulators and investors, in managing the risk that access to energy is lost. We further argue that adequate protection results from a hierarchical political decision process and is defined as compliance with a specific set of regulatory rules. Engineers inform politicians and economists so that they can judge the level of protection citizens want, within a framework intended to maximize social welfare, and truthful risk information must be shared among all stakeholders if that framework is to work. We conclude that regulations protecting citizens' access to energy are necessary and should balance their cost to citizens against an agreed probability that access will be lost. Although other models are possible, we argue that a public utility commission with the force of law is probably the best vehicle for setting the rate structure and the return investors earn on regulated costs.

Preamble: politics, engineering, energy, and social welfare

Access to energy is necessary for human survival. Society must produce and distribute electricity, along with stored energy sources such as oil and refined products, natural gas, coal, and hydropower, so that citizens can meet their vital needs: food production and distribution, heating and cooling against extreme weather, health care, clean water, communication, and more. Over several decades electric power has become one of the most essential of these energy sources, one

on which effectively every citizen relies. As a result, even short interruptions can have serious consequences.

The consequences of an outage depend on its circumstances and location. Large outages in the United States are uncommon, but they do happen and are sometimes sustained for long periods; the country covers a very large, and in places discontiguous, land area (see, for example, Hines et al., 2008). In a hospital, a sustained loss of power could cost lives almost immediately, so protection against it is taken very seriously: backup generators, independent power feeds, and similar measures make a local outage less likely where it matters most. Most private citizens, however, cannot afford or accommodate backup power, so the great majority will lose power, to varying degrees, in a blackout.

A natural question is: to what extent should citizens be exposed to losses of electric power? The answer lies in managing social welfare. In their 2017 paper "Protective Systems: Margins of Safety, Regulatory Authority, and the Calculus of Negligence," Wortman et al. (2017) derived a framework for maximizing social welfare and showed that welfare is maximized at the point of minimum cost found *within the regulatory framework*.

The role of *protective systems* is to manage the likelihood of consequential events over the lifetime of a technological system such as the public electric grid. They detect disruptive events and activate controls that make a loss of supply less likely. Protective systems do not increase an enterprise's revenue; they limit the costs of lost production, such as liability claims and collateral harm. And collateral harm occurs only when a protective system fails or was never provided.

1 Why protections?

For millennia, people have built technological systems of increasing complexity to overcome, or at least escape, the harms nature presents. Winter cold calls for shelter and energy; pests and drought destroy crops; moving goods over mountains, valleys, and rivers requires transportation infrastructure; medical devices and medicines fight disease and mend broken limbs. But people who rely on these systems can be harmed whenever, for any reason, their benefits are withheld.

Consider figs. 1 and 2. A narrow view of a technological system—one that provides electric power, for example—treats it as a "black box" that takes inputs, operates on them, and produces outputs (fig. 1). We take a more detailed view: however simple it may appear, a technological system is made up of interdependent subsystems, and subsystems within subsystems (fig. 2).

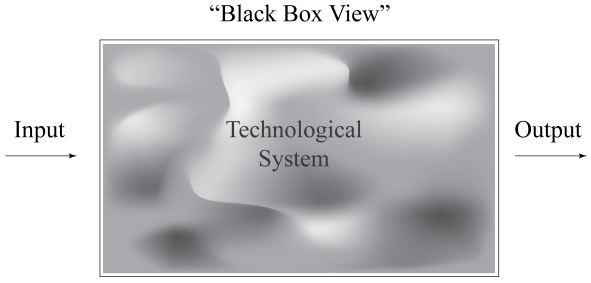


Figure 1: An integrated view of a technological system, in which its subsystems are hidden and it is seen only as taking inputs and producing outputs.

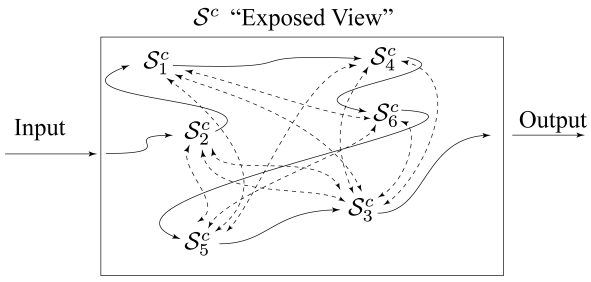


Figure 2: A technological system seen as a collection of subsystems that work together to turn inputs into outputs.

Where regulation requires it, another kind of technological system—a protective system—is added to the production system as an "overlay" (fig. 3). It acts as an attenuator, cutting off the progression of harmful scenarios such as those that would cost citizens their access to electricity.

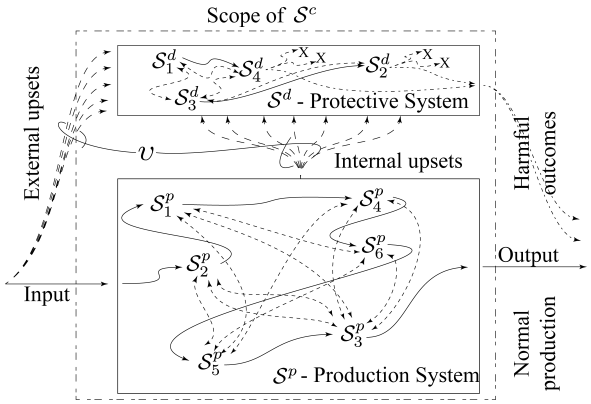


Figure 3: A technological production system with a protective system shown as an overlay. The protective system attenuates most upsets that could otherwise lead to harm.

We focus on the protective system, and in what follows explain why we treat it as separate from the production system it overlays. In general, a protective system exists to respond to upsets to normal production, shown as υ in the figure; upsets arise both within the production system and outside it. In our view, the scope of a protective system is comprehensive. It includes

1. all sensing technology used to detect upsets in operation;
2. all equipment and personnel responsible for responding when an upset is detected;
3. all emergency response equipment and personnel, public and private; and
4. all management infrastructure, public and private, that governs how protective systems are designed, deployed, operated, and regulated.[1]

[1]This definition of the scope of protective systems was first presented at the American Nuclear Society's PSA 2017 conference in Pittsburgh, Pennsylvania.

2 Regulated elements of protection

Regulation provides *ex ante* protection in the form of safety rules that are enforceable as law and must be followed to do business legally. Those rules are limited to the design and operation of the protective systems that overlay a production system. An immediate consequence of regulatory oversight—requirements, inspection, and enforcement—is that compliant businesses incur costs for protections they would rather not pay for. That is not to say that companies operating power plants would forgo all safety-critical protections; some level of protection does enhance the value of an investment. But profit-seeking investors are not the only economic stakeholders. Citizens benefit from access to energy at a reasonable price and are harmed when it is withheld, yet they have no share in the profits. Government addresses that imbalance in part by imposing protections in advance through safety regulation.

One might ask why regulation is needed if citizens understand and accept the risk of harm.[2] But citizens rarely, if ever, have the information that investors receive from the engineers, scientists, and lawyers they employ. Citizens are also typically more averse to risk, since they have more "skin in the game." That mismatch in information and in appetite for risk is what justifies government oversight of electric supply. Regulators act as citizens' proxy in understanding and assessing safety, and they set the safety requirements they judge to be in society's best interest.

Definition 1. *A* safety-critical protective system *is a collection of physical and human resources, engineered and managed to mitigate the consequences of upsets in the operation of energy production technologies.*

The term *safety-critical* applies to a protective system that overlays the production technology. Safety-critical protective systems therefore safeguard citizens who rely on energy technology and could be harmed if their access to energy were withheld. They act as filters, designed both to anticipate and recognize the start of a disruptive event and to mitigate its potentially catastrophic consequences. Our concern is to understand how effective the protection they provide actually is.

3 Adequate protection, critical infrastructure, and regulation

> *"If I ordered a general to fly from one flower to another like a butterfly, or write a tragedy, or to change into sea bird, and if the general did not perform received order, who would be in the wrong, him or me?"*
> *"That would be you," the little prince said firmly.*
> *"Exact. We have to ask from everyone what everyone can give," resumed the king. "Authority is based on reason. If you order your people to throw themselves into the sea, they will make the revolution. I have the right to require obedience because my orders are reasonable."*
>
> (Antoine de Saint-Exupéry, *The Little Prince*, 1943)[3]

The expected result of regulatory oversight is that the owners of production systems will design, deploy, and operate compliant safety-critical protections. For the individual consumer, however,

[2] The Coase theorem addresses the relationship between regulation and property rights where economic externalities are involved.

[3] English translation from Classica Libris, Kindle edition.

the reliability of the electricity supply and the terms of service are matters of contract. Left to the supplier alone, those terms will protect the producer from losses due to interruptions that can reasonably be called beyond its control. Extreme weather, volcanic eruptions, earthquakes, extreme flooding, pandemics, and other rare but consequential events are typically not covered by the service contract. That raises the question: who should pay for protection against such events?

Protective systems cost money, and it is reasonable to assume that their effectiveness increases with what is spent on them. But effectiveness has an upper limit, so each additional dollar of protection buys less. The cost of protection also affects stakeholders differently:

1. *Investors'* profits are reduced by regulated protections. Protections must be paid for with capital that could otherwise go to production, which raises costs, forgoes potential revenue, and so steadily reduces profit.

2. *Citizens* face steadily higher prices as the cost of regulated protection rises, and higher prices effectively reduce their access to the product.

3. *Citizens*, however, also face steadily smaller expected losses from losing access to energy as spending on protection rises, so their satisfaction increases with investment in protection.

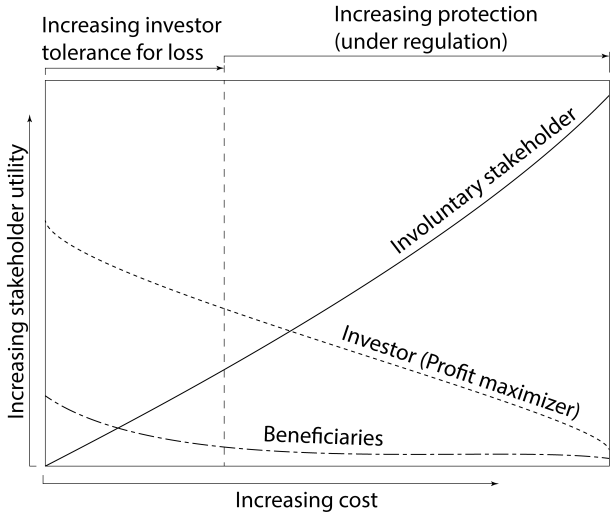


Figure 4: A notional view of how expected utility varies with the cost of regulated protection, as perceived by investors, citizens, and beneficiaries.

Plotting satisfaction (utility) against the cost of regulated protection for a typical member of each group gives the monotone curves in fig. 4. The figure also includes "beneficiaries," citizens who for various reasons are less exposed to harm from outages—for example, those who can afford their own backup generation, or who have "off-grid" alternatives for services that depend on electricity, such as drinking water and sewer service. Regulators understand these competing interests and must write rules that constrain the design of safety-critical protections. Those constraints largely benefit risk-averse involuntary stakeholders at the expense of risk-neutral investors and nearly risk-neutral beneficiaries.

Regulators typically do not design the protective systems they oversee. Instead, they set rules that constrain which designs are acceptable, and the designs themselves are developed outside the agency. Because regulatory authority is limited to rulemaking and enforcement, companies operating power systems are free to seek the most profitable design within the space the rules allow. When rare external events can cause an extended loss of power, it is the job of elected officials to enact laws from which regulations follow to protect citizens from harm.

Maintaining electric supply also requires keeping demand and production in balance, because electricity can be stored only in relatively small amounts. Once demand exceeds supply, the grid operator must curtail power according to the customer contracts in place; businesses generally negotiate lower prices by agreeing to be curtailed first.

Statutes nearly always prohibit regulators from writing rules that rely on monetary measures.[4] "Adequate protection" is therefore defined by rules that do not directly consider either the cost of protection or the cost of losing power. Investment in electric generation, on the other hand, requires a return, and that return must come from the price of electricity.

4 Design as decision-making

Designing protective systems, like all engineering design, is an exercise in decision-making. Regulators seeking adequate protection will, in principle, rank alternative sets of rules and choose the set they most prefer for achieving it. Designers and operators of protective systems will in turn rank alternative compliant designs and build the one they most prefer, typically the one that maximizes expected profit. Regulators and designers exchange information and analyses almost continuously. That open discussion, though sometimes criticized as a path to regulatory capture, ensures that both sides hold the same information about what adequate protection requires.

Adequate protection is thus the outcome of a hierarchical decision process: regulators choose their preferred set of rules, and the regulated company responds with its preferred protective design. There is no single composite measure of adequate protection that could serve as a threshold for compliance. Adequate protection is simply compliance with a specific set of regulatory rules.

5 Discussion

A large electric grid requires a close balance between supply and demand. Small imbalances can be absorbed by adjusting voltage or frequency, but such "brownouts" should not last long. If the imbalance grows too large, businesses and citizens must be dropped from the grid until balance is restored.

One possible protective system, with the force of law, would require generators to maintain enough reserve capacity that, if production is lost to an external event, balance can be restored by ramping up the reserve. Maintaining substantial capacity beyond what can normally be sold

[4] Sven Ove Hansson's 2004 article "Philosophical Perspectives on Risk," *Techné* 8(1): 10–35, implies this as a moral imperative in his Rule 5: "Nobody should be exposed to a risk unless it is part of an equitable social system for risk-taking that works to her advantage."

is not, by itself, a reasonable business proposition. Yet citizens are clearly harmed when they lose the power they have come to rely on. A regulatory mechanism such as a charge on electricity purchases would therefore make sense, to cover the cost producers incur in keeping a ready supply available for when the grid falls out of balance. That reserve should be tightly regulated and regularly tested, so that it is ready when an upset requires it, and its design, operation, and maintenance should be regulated in a way that fairly compensates the producers who provide it.

6 Summary

Protective systems overlay production technologies to limit the harm that operational upsets could cause. Their elements are regulated to ensure *ex ante* protection where vital services, such as access to electricity, could be withheld. Regulation focuses on the effectiveness of protection, not on the production process itself: regulators set rules that constrain the design of protective systems.

Protection serves citizens directly by guarding them in advance against collateral harm. Regulators are charged with setting the rules whose satisfaction defines adequate protection, so a compliant protective system provides adequate protection by definition. Private companies under regulation must be able to earn a reasonable return on any generating capacity they are required to hold beyond what they could sell under normal conditions.

Finally, the public good lies within the province of our political system. Legislators represent the public good by enacting laws that regulatory agencies are then given the executive authority to carry out and enforce.

References

Hines, P., J. Apt, and S. Talukdar (2008). Trends in the history of large blackouts in the united states. In *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, pp. 1–8. IEEE.

Wortman, M., E. Kee, V. Moiseytseva, F. Yilmaz, and D. Johnson (2017, September 24-28, 2017). Protective Systems: Margins of Safety, Regulatory Authority, and the Calculus of Negligence. In ANS (Ed.), *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2017)*, PSA, Pittsburgh, PA. American Nuclear Society: American Nuclear Society.