[24]

IS IDIOT PROOF SAFE ENOUGH?

Louis L. Bucciarelli

Introduction

"Idiot Proof": a phrase heard often enough in the design process, meant to convey an imperative of the design—it ought to be made such that even an idiot can work it, and, for the purposes of this paper, to work it safely. Indeed, justification for this design stance is often given in terms of safety: If participants in design do not attempt to foresee and guard against any and every possible dangerous misuse of the product, no matter how idiotic, the firm may be found liable for damages.

So we shield the innards of our machinery from the user, we multiply internal redundancies, and add "idiot lights" to inform and direct the user to take appropriate action; e.g. call the service department, if something doesn't appear to be working. By design we insure that our user can only act as idiot; he or she has no other recourse.

This espousal of human incompetence reflects not just a belief prerequisite to safe design but an ideology that pervades the whole design process, one that defines certain ways of doing and evaluating design as legitimate and rules out others. Setting rigid and impermeable interfaces with potential users is one part of the scheme and as such reveals the designer's desire to maintain control over both the design process and over the design, the artifact itself. It is not a contradiction to argue that, while safety considerations may justify "idiot-proof" design, an "idiot-proof" ideology may work against safety.

I first set the stage with a discussion of uncertainty in design. I then discourse on the way we attempt to cope with uncertainty through rational artifice and ask in a rhetorical manner, if this, by itself alone, can insure safe products. Playing off the significance of uncertainty against

Louis L. Bucciarelli is an Associate Professor of Engineering at the Massachusetts Institute of Technology and a participant in the Program in Science, Technology, and Society within the School of Humanities and Social Sciences. *For the past five years he has been engaged in a research program on Values in Engineering Design, an effort supported in part by the National Science Foundation. This paper "Is Idiot Proof Safe Enough?" derives from that investigation.*

the rationality of factors neatly arrayed leads me to a quandry, of my own making of course, out of which I will emerge with an alternative description of design as practiced, which then leads to my conclusion. Is idiot-proof safe enough? No, or at least not necessarily.

Uncertainty

Uncertainty in design exists in more than one guise. Uncertainty about what the user might do with the product, what foolish moves might be demanded of the artifact, is one form. But uncertainty permeates the whole design process every step of the way. It is what gives life to that process, what makes engineering the challenge that it is. The paradox is that in process we continually strive to banish uncertainty, to make it certain, to "freeze the design," as we must if it is to be realized.

The technical literature customarily makes a distinction between uncertainty and risk, i.e., the former qualifies features of the design, imagined scenarios of use, that are recognized as possible but about which one has little if any information about their probabilities of occurrence. Risk, on the other hand, quantifies the possible and gives the designer more to grab onto.

There is another category: "the un-thought-of." The un-thought-of is ignorance, the unknown, even unknowable. In design, we lack any markers, references that locate the unknown *vis-à-vis* the other ingredients of design. Unthought of, unknown, unimagined—for to imagine is to image, to already give shape, in part to define, to make *un*certain. Uncertainty, in all of its forms, permeates design, How to cope with it is the challenge, a challenge that gets explicit recognition when safety is the issue. "Idiot Proof" is an expression of one way to cope. Yet only an idiot would claim that his or her design accounts for every possible use or misuse. The unknown, the uncertain goes "out the door" with the product.

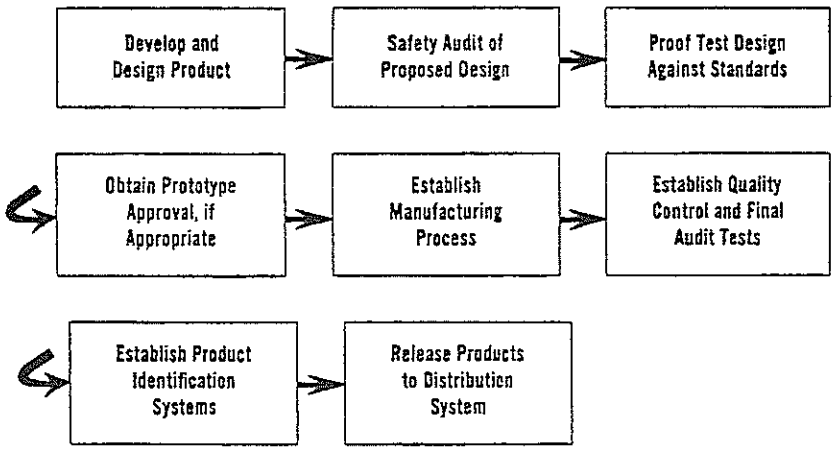
Coping With Uncertainty—Rational Design Programs

No longer is "caveat emptor" a sufficient response to the challenge of design for safety. Like Henry Ford's marketing philosophy, "let the buyer beware" stands as an attitude of the past. This is not to say that it fails to sustain the beliefs and norms of participants in design in some ways, nor do I intend to ignore the positive qualities of such philosophy: Arrogance, yes, but there is an air of honesty about it too, a recognition that design can not accomodate all possible human abuse. Then too, it presumes an intelligent user, perhaps one who can read Latin.

But nowadays we designers assume a greater responsibility for the life of our artifacts. Our reach and our vision extend out into the

marketplace, into the homes of fools as well as the learned. The presumption is that we are more rational, we know more, know better now; furthermore we judge our technologies to be so complex we think it necessary, almost natural, to take on this extended responsibility. In fact, not to do so might be judged irrresponsible.

So we strive to think about and deal with safety in a "rational" way. We construct instruments and charts, weights and measures, and plot our course through design. Supposedly objective, disinterested technique frames and guides our design concepts and decisions. We are all familiar with the block diagram showing the flow of the design process:



The designers of these maps attempt to break up into manageable bits and pieces, what is in truth a complex, diffuse social process. They order and segregate the different functions that have to take place for design to happen, placing all the bits and pieces into boxes to limit and define their reach, then tie the boxes together with a network of directed lines to convey the impression of an orderly flow in time.

From the rational perspective of the block-diagram, well formed rules and regulations appear to guide all choice, to reign over all. Even the limits, the range of consumer behavior, however irrational, can be defined and a rational, safe product conceived.

Rational technique finds expression again in the lists of things, the steps designers ought to follow, to insure safe designs. In the same reference we read about a "System for Identifying and Evaluating Product Hazards" list, and a "Checklist of Some Hazard Sources" list, a "Checklist of Some Hazards Associated with Hazard Sources" list, a "Checklist of Some Man, Environment and Time Factors" list, and a "Checklist of Some Factors

Potential Failure of Malfunction Loss Exposures" including "wear, overload, aging, moisture . . . unrealistic service requirements, and loss of power" list.[1]

All of this apparatus is designed to insure that designers, especially in the first stages of the process, attend to safety in a comprehensive way. It is employed in an attempt to transform uncertainty into certainty by naming and listing imagined events, by constructing scenarios of failure, assigning probabilities to all contingencies, and estimating what they are worth.

These lists and diagrams, fault trees, and probability estimates, are rational, are believable but the whole pretends to be more than the sum of the parts. They are all constructions. Like castles in the air, the safety engineer creates something with apparent substance out of the improbable by following systematic procedures, filling in the boxes, checking off the lists. As the lists grow, as the categories range wider, as the branches of the tree bifurcate and fill up the page, as the significant figures multiply, we begin to believe we have a sure hold on the matter, that our vision is complete.

Like a playwright struggling with the fabrication of tragedy, the designer strives to construct a sequence of events that could lead to a disastrous climax. The imagined action or plot has to be believable, even if transacted by the technically illiterate, although, like the playwright, the designer can trust in the suspension of disbelief of his audience. The language of numbers weighs in mightily here.

It is the latter that separates designers from others who fantasize about uncertainty. Some op-ed writers for the *Times*, as well as commentators for the evening news, engage in the social construction of risk but their visions lack the hard detail and the neutralizing, dispassionate ambience conveyed by quantity. Critics conclude their play is folly, unconvincing, their plot without substance, disjointed, irrational. (Still it packs them in.)

Either way we are attending to fantasy. Though the safety engineer's production appears real, it is at root an imagined sequence of events (despite the significance of its figures). If their probability of occurrence is extremely small, no history can render it any more reasonable than the dreams of an idiot.[2]

The attempts to make rational what is so uncertain are attempts at control. But a price is paid through this reduction of the design task into supposedly independent elements to be managed by specialties. These pockets of discipline and places for rational action speak their own languages, constitute their own worlds. Like separated regions of yet one nation, they speak different dialects. The burden of synthesis then shifts to the boundaries between specialties and sub-systems, is loaded onto the edges. Interface constraints are where the action is, where the heat is generated and where uncertainty is most in evidence

"Idiot Proof" points to a particularly troublesome interface—that with the unknown user. As such it is an admission of lack of control, a bit of a sell-out to the non-rational. It also signals a lack of participation of the user in the design process. No negotiation transpires. No opportunity for feedback. So rational design says assume the worst, assume the user is an idiot.

This splitting up the complex and diffuse into simpler elements, has another consequence—it engenders the belief in the independence of the elements, of the things named. We find ourselves in the land of "trade-offs" where safety trades-off, competes with other design requirements, usually low cost, efficiency, or productivity. It is no wonder then that safety is perceived by design practitioners as an add-on and that safety becomes a task for the safety engineer alone, a subject for discussion at the safety meeting and little explicit attention elsewhere. This need not be, for it is but a consequence of our design of design.

Coping With Uncertainty—Conservative Design Practice

The rational design program is itself an artifact, a construction intended to guide design, one rooted in a particular system of beliefs, hence not necessarily unique. It also fails to describe the real process. It leaves important stuff out, stuff like the unknown, the unnamed, stuff like the way participants in design stumble around in the quasi-dark, modeling, estimating, negotiating, procrastinating, staying up all night, etc., and it ignores the fact that design is a social process. That is clear. Go into the firm, listen to conversation, negotiation, laughter. At formal and informal gatherings of twos and threes, of more, participants work to construct shared meanings, to agree on what is important, what is critical, where to move next. Consensus is signaled sometimes by a formal memo, more often by oral affirmation. Bit by bit, step by step, design proceeds, concepts evolve.

Uncertainty from this perspective takes on an added dimension: no longer is it just a matter of a designer unable to estimate or even imagine the shape of the future but now he or she must deal with the ambiguity of a multitude of different perspectives and visions of the future. Uncertainty now has an immediacy about it—it permeates every discussion among participants.

So participants struggle to communicate, to plan, to maintain control. They work to know the technology they prescribe, to develop an adequate relationship with the stuff, to be able to anticipate its workings completely, including its possible failings. They must come to know it as object, as function, its special quirks and features; know enough so that they know when they have a marginal design, when they have a robust design. But there always still remains the unknown, more to know. And

they must convince others within their group, others at the interfaces, still others further afield, that they know enough.

Design process in practice is a conservative affair. The nuts and bolts, the stuff of hardware, requires the designer to know it on its own terms. There are no facile arguments, however eloquent, that will have nature behave counter to its character, however strongly we might will that to be so.

Conservative design doesn't accept the authority of abstraction, of number, of rules and of codes as complete. Rational plans and procedures will not suffice. As useful and as necessary as these techniques may be, they are not sufficient to insure quality of design. The design practitioner relies heavily on tradition, on what worked last year, then presses further, strives to know the material thoroughly so as to be able to predict how the design will function in all circumstances. There is a negotiation process going on here—between the object and the designer. The designer seeks to establish full control; there must be no surprises but that sense of control comes from a mastery of details, details not necessarily articulated as elements of a list or as quantities that sum.

Conservative design practice rarely gets the glossy articulation that the rational design programs receive. It doesn't have the same respect. Yet designers acknowledge and affirm it in the way they actually do their work. Sometimes there are clues in the phrases one hears . . . " not invented here" . . . a phrase reflecting a reluctance to accept a technique that doesn't grow out of a conservative process on one's own turf. "Idiot Proof" is another.

Individuals who espouse conservative practice in public, outside the firm, are rare: Admiral Rickover is one lone figure worthy of quote. In the record of Hearings before the subcommittee on Energy Research and Production, Committee on Science and Technology, US House of Representatives, May 1979, hearings held in the wake of the accident at Three Mile Island, he states straight off:

> First, in any engineering endeavor, and particularly in an advanced field such as nuclear power, conservatism is necessary so as to allow for possible unknown and unforeseen effects.

The unknown and unforeseen, not the uncertain or risky. There are no probability estimates tacked onto phantom events here.

Later in his testimony, when pressed by a legislator about the possibility of a reactor core melt-down, Rickover appears not to understand the question. His reaction is not an evasion but rather a refusal to acknowledge the relevance of probability estimates to the task of producing a high quality design of a nuclear power plant.

Further evidence of Rickover's disdain for relying upon rational design instruments alone in the design and management of complex technology is revealed in the following lengthier quote:

> One of the elements needed in solving a complex technical problem is to have the individuals who make the decisions trained in the technology involved. A concept widely accepted in some circles is that all you need is to get a college degree in management and then, regardless of the technical subject, you can apply your management techniques to run any program, including the Presidency, Congress, or the Vatican. This has become a tenet of our modern society, but it is as valid as the once widely held precept that the world is flat. Properly running a sophisticated technical program requires a fundamental understanding of and commitment to the technical aspects of the job and a willingness to pay infinite attention to the technical details, I might add, infinite personal attention. This can only be done by one who understands the details and their implications. The phrase, 'the devil is in the details' is especially true for technical work. If you ignore those details and attempt to rely on management techniques or gimmicks you will surely end up with a system that is unmanageable, and problems will be immensely more difficult to solve. At Naval Reactors, I take individuals who are good engineers and make them into managers. They do not manage by gimmicks but rather by knowledge, logic, common sense, and hard work and experience.

Intimate knowledge of and "infinite attention" to details, a struggle to know thoroughly and thereby have control over a design, this is at the heart of conservative design practice. For the Admiral, it applies to the management as well as the design of reactors. The phrase "idiot proof" doesn't appear anywhere in his testimony. His designs are meant to be managed by competent operators, individuals able to learn, to come to know the details.[3]

The antithesis to Rickover's approach is reflected in an article by W.E. Norquist, of the Polaroid Corporation, who, at the time of writing, was Director of Quality Assurance and Reliability. After urging that the design engineer take full responsibility for making a reliable and safe product, he goes on to state:

> Companies often expect too much of the user. The best way to minimize problems [of reliability and safety] . . . is to reduce the part [the user] has to play . . . When a consumer's part is reduced by designing him out, he will become more critical of any lack of performance. This means that the efforts to improve reliability can themselves create pressures for even more reliable products.[4]

Norquist recognizes that there is a penalty to pay for "designing the user out" of the system—the design must be ever more reliable. With the consumer barred from the details and intricacies of the design, if there is a mis-function, albeit even a trivial lapse in function, he or she is liable to become more critical of performance. Hence the need for additional redundancies, to attend to more details.

Yet there will always remain the unknown, the uncertain, the unaccounted for. With the user "out of the loop," shielded from the details of the device, there is less possibility he or she will act rationally, judiciously, if the unaccounted-for weighs in. Rather, as Norquist suggests, the user might react in frustration. Or perhaps he or she might choose to ignore the atypical if operations allow. At any rate, the potential for aliena-

tion is high. For the user with no access to the artifact there is no way to explore, to learn about the design, little possibility to maintain, or interpret its workings beyond what the documentation describes.[5] The wall erected at the interface, together with the increased sophistication of all the machinery required to insure the reliable functioning of the artifact in the hands of an idiot, insures that the user remains just that.

Conclusion

"Idiot proof" reflects the design participant's need to maintain control over the design; a thirst to know it thoroughly, to be able to predict and insure its proper function under all conceivable conditions, even when subjected to the misguided moves of a blundering, un-informed user. The effect is to forbid trespassing within the world of design. As such, the designer's intent may appear to be to protect the design itself from tampering as much as to shield the user from harm.

Freezing the user out of the system leaves the user with but the simplest, routine kinds of choice to make in the day-to-day operation of the technology at hand. Consequently if an unforeseen situation arises and presents an odd constellation of signals to the operator, his or her reaction is liable to be counter-productive, even destabilizing, if there is no room for the exercise of intelligent judgment and independent action. In this respect idiot proof is not safe enough.

FOOTNOTES

1. "Safety in the Marketplace, A Program for the Improvement of Consumer Product Safety," National Business Council for Consumer Affairs, Sub-Council on Product Safety, U.S. Dept. of Commerce, April, 1973.

2. Might this rational elaboration of disaster constitute a self-fulfilling prophecy? Any constraint, any bounding, or limiting condition on design, guides as well as restricts possible concepts and shapes allowable design thought and practice. If someone proclaims that two new cancer deaths per 2000 reactor years is the limit, someone else will design a reactor to take us there.

3. At another place in his testimony, Rickover argues for the value of simplicity in design. This too is a tenet of conservative design practice—"keep it simple for safety."

4. W.E. Norquist, "How to Increase the Reliability of Consumed Products," *Mechanical Engineering*, January, 1973.

5. The problem of writing good documentation is notorious. In its attempt to remain free of ambiguity, mystery, to be perfectly clear, it too treats the reader as simpleton. Of course it dare not suggest that the artifact might surprise the user on occasion.