

COPYRIGHT NOTICE:

Constance Perin: Shouldering Risks

is published by Princeton University Press and copyrighted, © 2004, by Constance Perin. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers. Follow links for Class Use and other Permissions.

For COURSE PACK and other PERMISSIONS, refer to entry on previous page. For more information, send e-mail to cope@MIT.EDU.

Preface

The Culture of Control

SHOULDERING RISKS their designers have foreseen, bullet trains, jumbo jets, manned space capsules and stations, nuclear power plants, offshore oil rigs, and supertankers deliver services, goods, and knowledge we have come to rely on. Heroic in their ambitions, in the amazing materials making them possible, and in the immense amounts of money and the millions of people mobilized to design and operate them, these technologies maintain uncanny control over gravity, friction, and temperature to defeat known dangers. Their size, reach, beauty, and raw energies awe us. When accidents take or threaten lives and destroy or degrade ecologies, awe turns to anxiety, horror, grief, and mistrust. Wary of that possibility, designers devise worst-case scenarios and try to preclude them. Although that reduces the odds of accidents, the outcomes of any one are likely to be major—hence, “high consequence” or “high hazard” technologies, as they label themselves.

Shouldering risks no one has foreseen is left to those standing watch on the bridge between designers’ intentions and how they are being realized. Even with wide safety margins and detailed operating procedures, missteps, missing resources, miscommunications, or mistakes have to be found and put right before they can turn into a tragic flaw. More often than we hear about, and most of the time, those responsible for handling risks—boards of directors, engineers, executives, managers, operators, regulators—defuse worrisome situations, prevent surprises, and keep any that appear from becoming more serious.

Even so, short of an accident, missteps can have “high consequences” for public trust and for productivity. Testifying in October 2003 to their inability to stave off eight “severe incidents” in “just the last few years,” presidents and other executives of nuclear utilities in Hungary, Germany, Japan, United Kingdom, and the United States told an audience of about four hundred “how their organizations descended unperceived into a situation where both plant staff and management failed to see disaster lurking.” After “the degradation in safety was revealed,” repairs and lost revenue cost “hundreds of millions and even billions of dollars.” At this biennial meeting of the World Association of Nuclear Operators (WANO), whose theme was “transparency and openness,” the audience “sat spellbound as

their peers described, with the bitter benefit of hindsight, how this could happen, even to organizations that were once seen as industry stars,” *Nucleonics Week* reported. Formed in 1989 as a global response to the 1986 accident at Chernobyl, WANO provides members with peer assessments and technical assistance. “The world nuclear power industry is in danger, threatened by the negligence and complacency” of those companies that “had not heeded earlier signs and, in many cases, are still suffering the financial, social, and political consequences,” WANO executives cautioned at this Berlin meeting.¹

The reasons for these incidents, utility executives and WANO peer reviews said, were “negligence in cultivating a safety culture due to severe pressure to reduce costs following the deregulation of the power market”; not “paying attention to detail”; taking “safety culture for granted”; “overconfidence”; “production bias”; ignoring “significant operating experience”; engineers’ “arrogance and complacency”; safety plans without “follow-through.” WANO’s chairman Hajimu Maeda “warned that even if the public understands that nuclear energy has advantages, ‘that is not the same as public acceptance.’ ”²

“Transparency and openness” are certainly remarkable and welcome in an industry not known for plain public speaking. Those reasons nevertheless recite a litany I have been hearing since 1990 when, as a member of a research group at the Massachusetts Institute of Technology and as a total outsider to this industry, I began to study the kinds of knowledge and ways of thinking its experts bring to bear in reducing operating risks.³ By 1996, I had been invited into eleven nuclear power stations and a few utility headquarters in the United States and abroad, and to national and international industry conferences and technical workshops. I also had joined two teams of experts on invited peer visits at two plants abroad, under the auspices of the International Atomic Energy Commission (IAEA). From men and women who are chemists, control room operators, design and system engineers, electricians and electrical engineers, executives, health physicists, human resource managers, line and middle managers, maintenance supervisors, occupational safety specialists, outage managers, risk analysts, station managers, and others, I heard what “operating safely” means to them and saw how they try to improve the ways they do that.⁴ More recently, at three other U.S. nuclear power stations I revisited four events occurring a few months earlier with those involved in them and in analyzing them. Of the many kinds of feedback that control relies on, experts’ self-studies crystallize their understandings of how and why control is lost, recovered, and maintained.

Although not classified as “severe incidents,” the reasons for these events not only echo that litany, but they also reveal a pattern long a concern of the nuclear power industry, its regulators, and the public. After

analyzing an event designated “significant” for somehow threatening reactor safety margins, experts’ best intentions to prevent repetition or further trouble go unrealized too often for comfort, theirs and ours. Standard practice is for an internal team to drill down to a “root cause,” elaborate on “contributory causes,” and, through reverse engineering from the unwanted outcome back through its inputs, develop recommendations to prevent recurrence. Annually, at plants in the United States and Canada experts make from two hundred to ten thousand self-reports of problematic conditions, ranging from housekeeping flaws to significant events, and of those, some thirty to fifty come under an internal review team’s scrutiny.⁵ With this high volume of self-reports and self-analysis, the industry expects to ward off surprises and preclude repeats.

But not all event analyses turn out to have been sufficiently thorough, nor are all recommendations effective or carried out. In thirty-seven events involving safety-critical systems at U.S. nuclear power plants between 1992 and 1997, not only had previous errors not been identified earlier, but failures to correct already known problems came to light. These gaps were four times more numerous than errors involved in the event itself, according to a study the U.S. Nuclear Regulatory Commission (NRC) published in 2001.⁶ In those same events, previously recommended changes not carried out contributed to 41 percent of them, and in about 20 percent, utility and plant managers had not responded to industry notices of equipment defects nor to recommended revisions in operating practices.⁷ The longer problematic conditions persist, the less predictable and controllable system interactions become. Risk estimates that calculate the probabilities of equipment malfunctions do not also calculate the probabilities that these self-defeating patterns will be present.

The chance discovery in 2002 of long festering erosion on the head of the reactor vessel at the Davis-Besse plant in Ohio (one of the incidents discussed at that WANO meeting) revealed those same patterns. According to after-the-fact scenarios of the damage this could have triggered, the NRC and the International Atomic Energy Agency calculated that its severity would match that of the accident at Three Mile Island (1979). These patterns appear in other risky technologies, as for example, in the space shuttle program of the National Aeronautics and Space Administration. In its inquiry into the 2003 loss of the *Columbia* shuttle and its crew, the Columbia Accident Investigation Board found issues in NASA’s work systems and analytic processes similar to those contributing to the 1986 *Challenger* accident.⁸

At the same time as the nuclear power industry has made fundamental improvements in reducing operational risks, those self-defeating patterns persist and the reasons for serious trouble remain the same, across national borders. That is what *Shouldering Risks* tries to explain, by asking

a back-to-basics question: What *kind* of problem is it to reduce the risks of operating a nuclear power plant? Early in my field studies, a station manager in the United States introduced me to about forty managers and supervisors at their “plan of the day” meeting. Unexpectedly, he added, “The reason I’ve welcomed her is that as a cultural anthropologist, she sees the things we take for granted around here in a different way. She might help us to do the same, so we can get even better at what we do.” Despite the strengths of this industry’s culture of control, I conclude, “getting better” is possible but not as a matter only of doing the same things better. To lessen the number of events occurring at all and to increase the frequency of sound analyses and effective recommendations—the most fruitful ways to prevent “severe incidents”—it is a more fundamental matter of reconsidering this industry’s culture of control.

Like any culture, it is an intricate system of claims about how to understand the world and act in it. In this high hazard world, technologists’ explicit claims pivot around the dynamics of control theory, meshed with productivity concepts such as optimization and efficiency, to produce protective bywords such as command and control, defense in depth, feedback, margins of safety, procedures, rules, system reliability, training. These technically correct claims before the fact cannot be the end of it, however. When the switch is turned to On and risks appear in real time, it becomes apparent that technologists do not—cannot—incorporate into their control calculations the contextual dynamics that inevitably accompany operations. That neglect is intentional, inspired by the goal of designing self-consistent, workable systems according to analyses and simulations that assure the lowest possible probability of an accident—workable, that is, under eventualities designers have imagined. A peopled technology operating in the world is, they claim, a source of variability and instability to be minimized by maximizing automation, standardization, and training. Once operating, when control is threatened or lost, however, assumptions underpinning those technical claims come to notice: assumptions about the relationships of humans to machines, models to reality, ambiguity to certainty, rationality to experience, facts to values. Those assumptions and the practices they support, *Shouldering Risks* proposes, are sources of persisting troubles and patterns.

To realize this industry’s original promises—to mute the divisive and deadly politics of oil and to squelch the harmful consequences of burning wood and coal—remains a goal of many here and abroad. For others, the risks of operations and of those throughout the fuel cycle outweigh those promised benefits. In any case, promises to shoulder the risks of nuclear power production cannot be confused with the ways they are being kept, here and now and for the lifetimes of current plants and of those being built. That fact is not lost on the thousands of scientists, engineers, and

industrialists worldwide searching for technical improvements to make good on them. At one U.S. station, however, an engineer sighed in frustration, “We’re technical people, but most of our problems are cultural.” To keep cultural promises—to turn “safety culture” into more than a catchphrase—far fewer analytic resources are at hand or called upon. Until up and running, risky technologies are sheltered from the influences of competition and downsizing, missing documentation and trend analyses, legal culpability and regulatory penalties. In designers’ thinking there is little room for such worldly matters; they surface as those frustrating “cultural problems” for owners, operators, and regulators.

For real-time operations, the concepts and methods of the physical and engineering sciences lack sufficient scope. When machinery develops flaws, people make mistakes, or unexpected situations arise and going by the book becomes irrelevant, maintaining control depends, at the least, on situational intelligence, foresight, and, above all, on the interpretation of signals of many kinds. But relatively little engineering thought or other intellectual capital has been invested in analyzing the contextual dimensions of risk handling and risk reduction, compared to that invested in estimating risk probabilities. That neglect is one consequence of a hierarchy of credibility at the center of this culture of control, which esteems evidence deemed measurable and discounts that which is not. As pervasive as that hierarchy is across many domains of practice, it can work against realizing the very aims of this and other high hazard technologies. Noting “sharp limitations in the current state of knowledge about how risk is handled in human organizations,” a British study group in The Royal Society calls for a more “robust knowledge base” for designing the “social and administrative” changes often recommended “in the aftermath of major accidents.” The “research map is a bit like the population map of Australia, with almost everything clustered round the edges and hardly anything in the central conceptual areas.”⁹ *Shouldering Risks* tries to fill in some of that vast space.

• • • • •

At the book’s center are three chapters in which those responsible for daily operations at three plants discuss four events. At Arrow Station, a complicated repair of a critical component in containment displays a panoply of control dynamics. Station managers considered this event to be so serious that they put three review teams to work, each with somewhat different aims. At Bowie Station, each of two unrelated events, brought on by seemingly simple mistakes of experienced people, display some of the industry’s demographic dynamics and its ambivalence toward the costs and benefits of outages for repair and refueling. At Charles Station,

what turned out to be an ominously dangerous situation, found by chance, reveals the practical consequences of distinguishing “nuclear” and “nonnuclear” “sides” of plant design and operation.

These chapters sustain three perspectives on the events: reports of event review teams that analyzed each for the record; verbatim insights and observations of about ninety experts’ excerpted from my transcripts of our taped discussions; and my queries, observations, and reflections on this and other kinds of evidence. Those, and my ordering of that evidence, represent my “different way” of seeing: concern with experts’ ideas, concepts, knowledge, language; with their ways of thinking expressed in everyday practices; and with their understandings of their working relationships. Taking off from experts’ reports and from their insights are excursions into wellsprings of the issues and themes they bring up, not to second-guess their analyses but to accumulate historical, technical, and conceptual sources of unrecognized elements in this culture of control. My excursions travel into the research of others and draw on my archive of other experts’ observations and experiences as reported at workshops, technical meetings, and peer reviews, as well as on my discussions at other nuclear power stations (chiefly Overton Station, whose operations I had previously observed through its different operational phases). Maintaining the integrity of each perspective extends the spirit of my station visits: a collaborative critique toward understanding. As an Arrow Station expert said, heatedly objecting to a team report that compared its event with one more serious, “Events never die, they live on to be misinterpreted in the future!” Or reinterpreted along different lines, as I do in my reflections and as readers will through their own frames of reference.

To set the stage, chapter 1, “Complexities in Control,” begins with brief highlights of the industry’s last twenty-some years. In the United States, that history culminated in 2000 in the NRC’s revised reactor oversight process, which reemphasizes industry self-regulation. Oversight and self-analysis both depend on two pervasive but often unremarked elements of any station’s culture of control. One I call the tradeoff quandary, an ever-present negotiation among priorities, resources, and risks, technical and financial. In the customary course of operations, managers and experts face the quandary frequently, but when repairs or an unacceptable condition might force the reactor off line, the stakes become more apparent. A second element is each station’s multiplicity of specialists and the continuing influence of the industry’s naval origins. Risk handling continuously raises the question of how well or poorly distributed, integrated, and credible specialists’ varieties of knowledge and interpretation are. The chapter ends with a description of the industry’s approach to event analysis and improvement initiatives and an overview of my research strategy. Chapters 2, 3, and 4 then revisit the events.

The last two chapters respond to that motivating question, “What *kind* of problem is it to reduce the risks of operating a nuclear power plant?” Both offer several concepts for characterizing the ways of thinking and kinds of knowledge that risk handling depends on. In chapter 5, “Logics of Control,” I examine the interplay of the calculated logics that estimate risk, the real-time logics of handling risks, and the policy logics that the tradeoff quandary uses and produces. A seemingly inevitable parade of self-contradictions, practical dilemmas, and paradoxes depends on and seeds those policy logics, such as the blame and penalties that can stifle information about trouble; the need for narrow specialties at the same time as systemic awareness is expected; the testing and repair that can introduce new risks; standardization and routinization that diminishes flexibility and adaptation. Not recognizing or not considering how to approach this infrastructure of conundrums itself can precipitate risk escalating conditions. That lived partnership of calculated, real-time, and policy logics comes clear in an unusually detailed study by cognitive scientists of control room operators’ actual work practices. I find there a general model of risk reduction, whose animating principle is as much in force as is the principle of command and control: the principle of doubt shadowed by discovery. Calculated logics and policy logics, based almost exclusively on that principle of executive control, carry the most weight, however. The one principle can readily accompany the other, but that hierarchy of measurable and unmeasurable or, as we say, hard and soft knowledge, puts a thumb on that scale. Adding heft are several constructs guiding the NRC’s oversight process.

That knowledge hierarchy pervades today’s culture of control. Chapter 6, “Intellectual Capital for Regulation and Self-Regulation,” proposes that crediting “hard,” “objective,” and “quantitative” knowledge and discounting “soft,” “experiential,” and “qualitative” knowledge have two consequences for reducing risk. One is to limit the scope of evidence event reviews consider: that can stymie effective recommendations for technical and nontechnical improvements alike. Another is to impoverish theories of risk estimation and risk handling in complex industrial systems generally. A mode of thinking about parts, components, and assemblies transferred from engineering design and testing methods into operations I call the parts template, together with the project template, another mode transferred from the construction phase into operating, can obscure interdependencies among parts and among specialists’ different kinds of knowledge. Those modes of thinking foster understandings of reactor technology as being little more than the sum of its parts, rather than as a peopled technology using and producing invaluable technical and contextual knowledge about its condition. The persistence of those patterns of ineffective or unimplemented changes owes much to that misapprehension.

The crux of reactor control is configuration control: keeping track of expectable interactions within a complicated, often opaque system and responding promptly to those not expected. Close coordination among many specialists' perspectives and knowledge is key. But, the three event chapters show, often vexed relationships among the kinds of knowledge and ways of thinking of specialists in design and in operations, in maintenance and in operations, in support services and everything else can impede exchanges. That compartmentalization has a prominent and negative place in this culture of control, affecting the adequacy of information and analysis. Again, constructs guiding the NRC's oversight process can exacerbate that, as can the generally low status of "maintenance" relative to other specialties. Although that status is a staple of the industrial world, in this as in other high hazard technologies, the analytic and practical contributions of maintenance specialists are as vital as any of those of others, as serious events and accidents keep telling us. To fleets of aging reactors that expertise is increasingly indispensable.

Shouldering Risks ends with a thought experiment for reimagining a culture of control grounded in an expanded system of claims: it does little more than acknowledge the depth and breadth of the culture of control already demanded by the inner work of operating at least risk.¹⁰ The ultimate goal is to create conditions more likely to increase the frequency of effective and implemented CORRECTIVE ACTIONS and decrease the frequency of events. The conditions would maximize specialists' exchange and analysis of information. That depends on maximizing the communicative, observational, and interpretive competencies on which configuration control depends. This is the kind of problem it is to reduce the risks of operating a nuclear power plant, this experiment proposes.

That problem is entirely cultural and entirely pragmatic: the tradeoff quandary centers on evaluating the significance of evidence bearing on "nuclear safety," a term with the specific meaning of maintaining the capacity to shut down the reactor without releasing radiation at levels harmful to employees and to the public. An officially designated "significance determination process" judges daily the extent to which any operating condition or activity affects that capacity. To acknowledge that process as a prime element of the culture of control, this thought experiment entwines an axis of meanings with the axis of functions along which experts' activities are now arrayed. That acknowledges equally the observational and interpretive work that safe shutdown requires and that the principle of doubt and discovery demands.

To imagine cultures of control focused as much on knowledge and meanings as on departments and parts recasts the kinds of work and competencies risk reduction requires. That suggests other criteria for conceptualizing work systems, for the contents of technical and engineering edu-

cation, and, no less, for the architecture of working arrangements and relationships. Worldwide, questions about competencies are timely: even now nuclear-related industries are short of specialists, including executives and managers.¹¹ Any next generation of nuclear power technology will confront that problem, as will another option also on the far horizon: new initiatives in the basic science of burning plasma offer the prospect of fusion energy technology, another hazardous source of ozone-friendly energy that some experts say may be possible by mid-century.

Shouldering Risks moves from an immersion in experts' insights to excursions into wellsprings of this industry's culture of control. To enter into this world at this level of specificity, is, I believe, a necessary step for reimagining its culture of control, and perhaps those of other risky technologies. That said, some readers may want to begin with chapter 1, choose one of the event chapters, and after reading chapters 5 and 6, return to the other two. The event in chapter 2 is apparently the most complicated, the two events in chapter 3, apparently the least, and in chapter 4, an event centers on the process of evaluating the significance of trouble.

• • • • •

Although nuclear power production is one among other industries in the high hazard category, its complexities and the public ambivalence surrounding it obviously set this technology apart. Around the world as of March 2004, 439 nuclear power plants were operating and being upgraded, 30 were being built, and 34 were planned or on order. After fifty years of the "atoms for peace" program, which President Dwight D. Eisenhower advocated after the Second World War, nuclear power plants are for the first time new, middle-aged, and old. Some present familiar risks, some that are new; some operate in relatively stable social, financial, and political environments, some in those less so. The world has long passed the point of debating only whether nuclear power plants should be built at all or built where proposed. With 439 operating plants, whether one favors this energy option or not, their safe operation is obviously in the world's best interests, as is safely decommissioning those beyond repair or otherwise shut down, and, not least, securely protecting the fuel cycle and disposing of its waste.

Operating commercial reactors 2004

United States 103, France 59, Japan 53, Russia 30, United Kingdom 27, South Korea 18, Germany 18, Canada 17, India 14, Ukraine 13, Sweden 11, Spain 9, China 9, Belgium 7; Bulgaria, Czech Republic, Slovakia, Taiwan, each 6. Between 1 and 5: Argentina, Armenia, Brazil, Bulgaria, Finland, Hun-

gary, Lithuania, Mexico, Netherlands, Pakistan, Romania, Slovenia, South Africa, Switzerland.

Under construction

India 8; Russia 6; Japan 3; China, South Korea, Taiwan, Ukraine, each 2; Canada, Iran, North Korea, United States, each 1.¹²

Planned or on order

Japan 13; South Korea 8; China 4; Canada 2; Argentina, Brazil, Finland, India, North Korea, Pakistan, each 1.¹³

Over the nearly twenty years since the 1986 accident at Chernobyl, the United States's 103 operating plants have come to meet about 20 per cent of the national demand for energy. Since 1991, the average capacity factor (actual output compared to potential output) has increased 40 per cent; as of 2002 it rose to 91 per cent.¹⁴ At the same time, the industry has been experiencing new kinds of financial risks as many states deregulate electricity markets. The NRC's revised regulatory regime, still being refined, is taking hold as utilities and stations continue to reduce staffing and budgets, experience mergers, and rely increasingly on contractors. All that has been accompanied by a shift to separating ownership of generating operations from that of electricity distribution. These changes come at a time when developing a "new generation" of commercial reactors remains high on the industry's agenda.

As "indebted to Descartes and Newton" as we are "for fine examples of well-formulated theory" on which science and engineering depend, says Stephen Toulmin, philosopher of science at the University of Southern California, "humanity also needs people with a sense of how theory touches practice at points, and in ways, that we feel on our pulses."¹⁵ For the many concerned with those touching points in this and other high hazard enterprises as they are today and being planned for tomorrow—executives and operators, legislators and investors, designers and scholars, shareholders and policy analysts, and for us as citizens—our task is to reimagine their cultures of control.

• • • • •

Consider *Shouldering Risks* an attempt at preventive maintenance: replacing an invisible cultural apparatus manufacturing a neglect of the world in which heroic technologies come to life. Once we dismantle and inspect that cultural machinery and prepare to reassemble it, we might begin to imagine how its design and operational arrangements would change with different claims relying on different assumptions. That would allow us to evaluate their consequences not only for reducing operational risks, but also for reconsidering the premises of the many institutions—educa-

tional, financial, governmental, legal—bringing high hazard technologies to fruition.

From inscriptions, relics, ruins, and scrolls we infer much about the claims of societies that built the ambitious artifacts of the past—amphitheaters, canals, churches, pyramids, ships, temples, tunnels. We are in a position today to know these things for ourselves, and to choose. This book is meant to help us think through how things *could* stand, what could be otherwise in a future in which high hazard technologies are vulnerable not only to what has already been foreseen but to what has become much harder to foresee at all.

Heroic technologies not only express the maturity of industrialization after its first 150 years. They also test that maturity. How can scientific, engineering, and financial sophistications bringing us so many marvels also become wiser in the ways of the world?