

# Our Ultimate National Insecurity

By

**Emery Roe and Paul Schulman**

National security has been a major issue in the current presidential campaign. Defending the nation against terrorist assault has been championed by every candidate. But a pressing national security problem has been left unaddressed by all the candidates so far. It is the precarious reliability of many of our critical services in electricity, water, health care, telecommunications, transportation and finance.

This is not just the trillion dollar crisis of having to repair our deteriorating roads, waterways or electricity lines. A more important issue is that many managers and operators of these systems are now forced to work at the edge of their performance capabilities. It is a reliability crisis that no one outside their organizations seems to care about. As one long-time veteran of the electrical industry recently observed to us: “the public doesn’t realize just how vulnerable they are”. This is a crisis that will not be solved by new roads, waterways and electricity lines alone.

Over the past eight years of ongoing research, we have witnessed firsthand what it takes to provide a service like electricity reliably, across one of the world’s most complex electrical grids, California’s. What is remarkable is how often electricity is provided just-in-time. Sure, plans and schedules are made, but so much can happen up to the last minute that the electrical system depends on the skill and judgment, and sometimes the everyday heroism, of a handful of middle-level operators and managers – people we call “reliability professionals” --who keep the grid as reliable as it is, 24/7, 365 days a year. We have good evidence that the same holds true for other critical infrastructures in water, transportation, healthcare and financial services.

Not only are managers and operators being asked to do more with less, but what they are expected to do—always be highly reliable—has moved beyond challenging. Over 85% of the nation’s infrastructures are privately owned and many changes are being introduced driven by

the demands of an increasingly competitive marketplace. New policies, technologies and software are being introduced to optimize efficiency and performance. It would seem hard to argue with these objectives. Yet many of these changes and the way they are being introduced impose risks to the systems they are trying to improve. Electrical grid and market restructuring in California offers a telling example. The economists, engineers, software designers and policy-makers at the heart of these changes, believed as designers that they understood electricity, as with any other infrastructure, through the formal principles of their disciplines.

What designers then and now do not fully understand is that their very efforts at improvement can seriously challenge the skills and experience of control operators to manage essential systems reliably and safely. First, important factors in the operation of these technologies, which are really networks linking many participants, cannot be captured in the formal models of analysts. In addition, many new software and hardware systems fail to work as intended. It is left to operators to fill in the gaps and cope with the glitches. On the basis of their experience they craft strategies (often called “workarounds”) to manage the design errors that inevitably accompany new policies, software or hardware.

We’ve been in the control room of the California Independent System Operator at the height of the California electricity crisis, during some of its highest summer demand days since then, and during the October 2007 San Diego firestorms and the latest firestorms over the last month. We were also in the room on the many more days that never made the news when a vital transmission line or generator suddenly went offline putting service and the grid itself in jeopardy. At no time did the men and women in the control rooms panic; instead they acted with great skill, dedication as well as surprising imagination and creativity to keep their critical systems operating. But we have seen them driven to the limits of their skills and to near despair and exhaustion by failures in hardware and software systems imposed upon them by designers and external “experts”.

Policymakers and CEOs see nothing wrong with constantly changing market strategies, technologies and regulatory rules. They are wrong. Some of these changes and interventions are threatening significant declines in the high reliability of the systems we depend upon. Surprisingly, many are being designed by lawyers, economists, engineers and policymakers who know nothing of the operational requirements it takes to manage for reliability. Some have

not spent one minute in our nation's control rooms but stand ready to prescribe for their improvement.

If we truly hope to safeguard the reliability of our infrastructures, we need to commit to support more than replace the skills and often hard won experience of their managers and operators. We also need professional ethics to counter the hubris of those who intervene in our infrastructures without currently being accountable for their mistakes. In the absence of a new approach, many technical, and policy fixes by these "experts" can be quite literally as threatening to infrastructure reliability as the terrorist assaults we are hoping to guard against.

(Emery Roe and Paul Schulman have done extensive research over many years into the reliability challenges facing critical infrastructures. Their findings are reported in their new book, *High Reliability Management: Operating On the Edge* just published by Stanford University Press.)