We read the daily papers mostly to find out what has gone wrong, and presumably to learn from the mistakes, faults, and problems or others-or, at the very least, to feel good about not being personally involved. At the Massachusetts Institute of Technology, in a seminar labeled "Failure of Human Systems," the not very surprising conclusion was drawn (among others) that a failure is often considered as shameful, as something to be suppressed, particularly if the failure is construed by the participants as a personal rather than as a project failure. Thus, it is understandable that many individuals who do "make the papers" are not happy about it.

When we conceived this special issue on "What went wrong?" we recognized the possibility that engineers and engineering managers might be reluctant to discuss unsuccessful projects with which they were personally connected. Colleagues warned us that engineers might point the finger at others, but would not talk for the record about failures close to home.

Fortunately, those dire warnings proved largely unfounded. Peter Goldmark, in the course of discussing the ill-fated EVR project (p. 95), told Spectrum staffer Rubinstein: "Above all, somehow you must have the guts to admit to yourself—and to others—that you made a mistake and have to make a fresh start...."

One cannot discuss failure, and, particularly, failure analysis, without discussing systems concepts. This is true whether hardware or software failures are at issue. An important inference to be drawn from this observation is that an efficient, accurate failure analysis can be carried out only if the analyst has good knowledge about the system in question; as a corollary, if he does, corrective action to improve system reliability is easier.

Stephen Ehrmann, of M.I.T.'s Center for Policy Alternatives and a participant in the aforementioned M.I.T. failure seminar, notes that failure involves a triad consisting of an action or event, a standard against which to measure the event, and a judge to measure the event against the standard. We might append to Ehrmann's statement the observation that, depending upon the relative latitude or ambiguity of the standard, the judge may be sophisticated or unsophisticated. And, obviously, the judge need not always be human; sometimes it can be a piece of test equipment. In many catastrophic system failures, no designated judge is needed—any lay observer will suffice (e.g., in the case of an airplane crash).

A more general definition of failure is provided by Thomas Sheridan, former president of the IEEE Systems, Man, and Cybernetics Society, as "a discrepancy between one set of events (typically hypothetical events, i.e., an ideal model or statement of intent) and another set of events (typically observations of actual happenings)." He points out that in some cases the "fact of failure" may be based not on an explicit criterion, but rather on a judgment in which the criterion must be inferred (e.g., in which events are significantly different in certain ways from some other events defined as successful arbitrarily).

For the purposes of this special issue, we shall be dealing mostly, but not exclusively, with hardware
system-type failures whose criterion for success or nonsuccess is relatively unambiguous. Thus, we shall be less concerned with determining that a failure took place than in determining why it took place. In such cases, the failures may be technical, or they may be economic. Technical failures may be related to variable characteristics (the system may not reach its design objectives, yet it still "works"), or to inoperable elements (overstressed or poor-quality components). Of course, more sophisticated systems may contain failed elements and still function, albeit sometimes in a degraded mode.

In any event, if failed devices or components are at the root of a system failure, one may set about to determine the reason why, and the mechanism by which the device failed. In his article on "The failure tracers" (p. 32), Roger Allan reviews the science (and art) of failure analysis. Included with that article are case histories in which failure "detectives" have traced a failure to its ultimate cause. By the time you've finished the article, it should be clear that reliability is not an absolute, but a characteristic that is related to mission profile. The article also suggests that, while a systematic approach to failure analysis is desirable, short cuts, and sometimes a bit of luck, play important roles.

Although other articles in the issue relate principally to hardware case histories, one of them does not. "Dollars vs. satellites" (p. 74), by Ellis Rubinstein, examines the budget-driven decision by NASA to get out of the communications satellite business, a decision that, in retrospect, seems to call for reexamination.

Finally, the article entitled "What ever happened to...?" (p. 97) takes a backward look at some of the techniques and/or technologies that once were expected to yield significant benefits to society, but which haven't, apparently, fulfilled their early expectations.

It is entirely possible that reliability experts may feel somewhat uncomfortable and/or unsatisfied in reading this special report, and we believe that is understandable. Spectrum selected the case histories not because they represent a simple, clear application of system design and analysis, or of design for reliability, or even of failure analysis: rather, they represent "real world" projects, with the attendant time demands, political pressures, budget constraints, and the like.

When we first proposed this theme, one reader advised us: "I doubt if anyone will learn too much from someone else's mistakes. Some of us don't even learn from our own." Despite his pessimism, we believe the "Monday morning quarterbacking" provided by this issue will contribute to the profession, and to mankind.
The Great Blackout of '65

Could the 'long night' happen again? What was learned from the dramatic six-state (plus Ontario) outage of November 9–10, 1965?

On Sunday, July 4, 1976, at 5:50 p.m., the lights began to flicker in Salt Lake City, then went out entirely. Police and fire departments, hospitals, and Salt Lake International Airport immediately switched to standby generators that were available for just such an emergency. However, radio and television stations were knocked off the air and many families that had holiday dinners in electric ovens had to rely on charcoal grills and dine by candlelight. About one million people in 65 percent of Utah, plus southwestern Wyoming, were without power from 1½ to 6 hours. The incident did not receive widespread publicity outside of Utah and Wyoming. After all, it was the Fourth of July and most of us were preoccupied with Bicentennial celebrations.

By July 6, Utah Power & Light Company (UP&L) announced that it had traced the cause of the widespread outage to a relay that malfunctioned in the switchyard of its Naughton generating plant near Kemmerer, Wyo. The relay tripped two 230-kV transmission lines that were carrying 675 MW to the company’s Ben Lomond substation for distribution to major load centers throughout the state. Other generating units could not make up for the lost generation, became overloaded themselves, and tripped out.

Eleven years ago, a relay was also the initial culprit in a power failure that has become known to history as the “Northeast Blackout.” Since that infamous November night when the lights went out in New York and New England, a variety of remedial measures have been taken to strengthen interconnected systems. Nevertheless, despite such steps as load shedding, computerized data collection and processing, automatic monitoring, emergency response procedures, and the formation of coordinating councils to monitor system reliability, the Utah event suggests that widespread (if limited in degree compared to the '65 failure) blackouts are still possible.

According to a UP&L spokesman, the July 4 outage was isolated to the Utah system only as a result of preventive measures taken since 1965. “Ten years ago, it would have spread to other western states,” he indicated. Load shedding did take place in Utah, but “everything went down anyway,” according to another source.

Gordon D. Friedlander Senior Editor

Underfrequency relays permit utilities to shed load when a system is perilously close to collapse. These blocks indicate the status of automatic load shedding programs of members of the Northeast Power Coordinating Council. Data are listed in megawatts (as of January 1, 1976). The percentage of peak load is shown in parentheses, and loads are peak for the year 1975. Relays are set to shed approximately 10 percent of load at 59.3 Hz, and an additional 15 percent at 58.8 Hz. Facilities are required to relieve 50 percent of the load manually within ten minutes.

Those interviewed regarding the outage prefer to emphasize that reliability measures eliminated cascading outages and minimized the area affected—even though most of the sparsely populated state of Utah went out.

Actually, many of the remedies effected since 1965 are nothing new. Indeed, load shedding to protect against low frequency is a concept that dates back 40 years. “Black start” capability in the form of separate generators and starters would also seem to be a common-sense necessity, but few generating stations in 1965 had this capability. It took an “unthinkable” contingency like the instability of 1965 to spur studies of less probable contingencies and their effects on interconnected systems. As a result, there has been greater coordination in day-to-day system operation and in the planning of future power systems, as well as a continuing effort to install the sort of protective equipment and interconnected systems that could have prevented the 1965 blackout. But the philosophy that characterizes these efforts must be termed one of minimizing the effect of a contingency, rather than out-and-out prevention.

The outage of the five 230-kV lines from Beck to trip this unfaulted line. The power flow on the disconnected line shifted to the four remaining lines, each of which, in turn, became loaded beyond the critical level at which its back-up protective relay was set to function. Therefore, the remaining four lines tripped out in cascade in 161 cycles' time (2.7 seconds).

The outage of the five 230-kV lines from Beck No. 2 separated the Ontario generation along the Niagara Frontier from the loads in the province. [Immediately before the disturbance, about 1800 MW of generation at the Power Authority of the State of New York’s (PASNY) Niagara plant was flowing east and south over the New York State transmission system.]

The Federal Power Commission’s report notes: “With the dropping of the lines to Toronto, the power being generated at the Beck plant and at PASNY’s Niagara plant, which had been serving the Canadian loads around Toronto (about 1500 MW), reversed and was superimposed on the lines to the south and east of Niagara. It was
this tremendous thrust upon the transmission system in western New York... which exceeded its capability and caused it to break up.

“The instantaneous result of the tripping of the lines from Beck to Toronto was the acceleration of the generators at Beck and PASNY-Niagara, with a sharp drop in their electrical output... The instantaneous drop in generation at Beck and PASNY, followed by a rapid buildup in electrical power output, resulted in putting the Beck and PASNY generation out-of-phase with most of the other generation attached to the interconnected transmission system...”

Since the output from Beck No. 2 and the PASNY-Niagara plant could not be handled by the remaining transmission system after the tripout of all five lines at Beck, the EHV transmission system was severed 0.9 second later with the stability-limit opening of the two 345-kV lines between Rochester and Syracuse, N.Y. Almost simultaneously, tie lines to the PJM (Pennsylvania-Jersey-Maryland) pool were broken both in the Niagara Mohawk area and in Brooklyn at the Con Edison side (Greenwood Station) of a connection with PJM at Staten Island.

At 1.33 seconds after the separation of the Beck generators from their loads, the two 230-kV lines connecting the PASNY plant at Massena with the 345-kV trunk lines that run from Niagara to downstate New York and to New England tripped out. This action simultaneously tripped out five of the 16 generators at Massena.

The generators at the Beck plant were not provided with relays to trip them out upon loss of a transmission line, since such a scheme would have been ineffective in the face of the large increase in inflow over the Niagara system, which would follow and offset the loss of the tripped generation. (The simultaneous loss of the five transmission lines to the north was considered to be an improbable contingency.)

Within 4 seconds after the initial tripout at the Sir Adam Beck station, most of the Canada-United States Eastern Interconnection (CANUSE) area east of the state of Michigan (Maine and a portion of New Hampshire did not lose power) was broken into four isolated segments:

1. The Ontario Hydro system was completely separated from New York and was badly deficient in generation capability.

2. The northern New York region, supplied by PASNY—St. Lawrence and Niagara Mohawk’s northern hydro sources, was isolated, but the remaining generation was able to carry loads in the Massena, Potsdam, Watertown, and Oswego areas.

3. The region in the vicinity of Niagara, on the U.S. side of the international boundary (Niagara-Dunkirk area), including the New York State Electric and Gas south central area, was separated from the remainder of the interconnection and had large excesses of generation.

4. The balance of the CANUSE area, including a part of upper New York, the New England systems, and the systems in the southeast New York region, was separated from the rest of the group but remained interconnected within itself. Michigan was temporarily separated from all but a small section of the Ontario Hydro system.

In the 4-second time interval following the initial disturbance at Beck, in which the PASNY and Niagara Mohawk systems had split, the upstate New York area,

Those councils-NPCC, NERC, etc.

On January 19, 1966, executives representing the electric utilities in Ontario, New York, and New England signed a Memorandum of Agreement that established the Northeast Power Coordinating Council (NPCC)—the first such organization to be created in North America. The agreement stipulates that the purpose of the NPCC is “to promote maximum reliability and efficiency of electric service in the interconnected systems of the signatory parties by extending the coordination of their system planning and operating procedures.” (At present, the 21 NPCC member utilities supply 98 percent of the electric energy requirements of the New England States and New York, plus the Canadian provinces of Ontario and New Brunswick.)

The Council includes an executive committee, three standing committees, and nine task forces that conduct studies of all important aspects of bulk power-supply reliability. The Council also employs a full-time technical staff, in addition to providing an effective vehicle for promoting the reliability of electric power supply within the large region it serves. NPCC acts as a forum where all aspects of utility coordination for greater service reliability can take place.

NPCC has developed an automated data bank for storing, maintaining, processing, and retrieving technical data relating to electric generating and transmission facilities of its members. Recently, it devised a method for assessing bulk power transmission system reliability by means of a probabilistic technique.

On a continuing basis, Council members report their future plans for the expansion of power-generating facilities and transmission lines to meet new customer needs. Forecasts of electric demand, and plans to meet such demand, are issued regularly.

Major transmission facilities have been and are being constructed by Council members to improve the reliability of the Northeast Interconnections. For instance, from January 1, 1974, to June 30, 1975, some 320 circuit-kilometers of 115/138-kV transmission, 112 circuit-kilometers at 230 kV, 580 circuit-kilometers at 345 kV, and 320 circuit-kilometers at 500 kV were installed.

After NPCC was established, the general concept was adopted in other areas of the United States and Canada: today, almost all systems in the contiguous 48 states, and four Canadian provinces, are members of one of nine regional councils. These organizations linked together in 1968 to form the National Electric Reliability Council (NERC) for the purpose of “further augmenting the reliability and adequacy of bulk power supply of the electric utility systems of North America.”

At the present time, following years of improved reliability, the possibility of future vulnerability to power failures is being raised by some experts. Last year, NERC published its report on the reliability and adequacy of the North American bulk power systems. In it, there is a warning that present generation reserve levels may quickly diminish as the general economy improves. The report states that “the reliability and adequacy of electric bulk power supply is threatened in some areas of the U.S. as early as 1978...”

The document also cites an increasing number of postponements and cancellations of major electric units, along with a “substantial decline in transmission” similarly affected.

For the power industry, the NERC document recommends a continuation in transmission development “to meet future needs and to provide the maximum emergency support during periods of short-term capacity deficiencies.” But, simultaneously, electric systems should “continue to investigate all possible options for augmenting generating capability, and ways in which emergency transfer capabilities can be increased.” Finally—and this may be the nub of it—all power systems should “reexamine contingency programs to permit the orderly curtailment of load in the event of future inadequacy of bulk power supply facilities or fuel shortages.”
result of this point of rupture, was still tied to the New England and southeastern New York areas. This situation created an instantaneous deficiency in the fourth segment of about 1100 MW.

Meanwhile, at Con Ed . . .

Sixteen minutes, 11 seconds, before the incident began at Beck, Con Edison was generating about 4550 MW and drawing 220 MW from its interconnections to meet a load of 4770 MW. At 5:16 p.m., the Energy Control Center in Manhattan noted a sharp surge of power into the system—lasting between 50 and 90 cycles’ time. This was immediately followed by a high outward surge of about 1300 MW.

For a brief period, there was the impression that the system was stabilizing back to normal, but the Con Edison generators—as well as those throughout the fourth segment—were unable to respond quickly enough to the enormously increased demand upon them from the north. There was a drop in voltage and frequency and, in a matter of minutes, one system after another in southeastern New York went down as generators tripped out. Finally, at about 5:27 p.m., almost all power in four bourgeois of New York City was lost. The “night of the long night” had begun.

Where were you when the lights went out?

If you were almost anywhere between Toronto and Boston or New York on the evening of November 9,1965, the chances are you were affected slightly or inconveniently greatly; the Great Blackout touched some 30 million people over an area of 207,000 km² (about 80,000 mi²) from eastern Ontario through New York State and much of New England for periods ranging from a few minutes to 13½ hours. (For the complete chronology and details of this dramatic event, see “The Northeast power failure—a blanket of darkness,” IEEE Spectrum, pp. 54-73, Feb. 1966.)

Had you been a resident or worker in New York City on that evening, you could have been caught aboard a peak-hour subway or commuter train—or between floors in an elevator of a high-rise building. If you were luckier, as was the writer (the lights failed in midtown Manhattan while he was waiting for his wife at the corner of 45th Street and Fifth Avenue), you might have made it to a nearby restaurant for a candlelight dinner, where you

The New York Power Pool

In 1968, Con Edison and six of the largest investor-owned utilities in New York State plus the State Power Authority—formed the New York Power Pool (NYPP) to further coordinate operating procedures and joint planning, and to build a power pool center. The NYPP Power Control Center at Guilderland, N.Y. (near Albany), began the coordination of statewide generation and HV transmission in February 1970. Along one wall of the control room is a curved status display board, measuring more than 24 meters in length by 4 meters in height. It is situated above and to either side of telemeter recorder panels. Two IBM system 370/Model 155 computers in a nearby room assist in coordinating the dispatching of power throughout the state on a “single-system” basis. Power control operators are on duty in three shifts, 24 hours a day.

The nucleus of all the systems, however, is the electric power supply; thus, quadruple redundancy of power supply systems is provided to ensure maximum protection against electrical outages. In this unusual redundant configuration, two separate feeders from two independent substations serve as the primary and alternate power supplies. If both feeders fail, then a 250-kW gas turbine-generator set furnishes emergency power. All three power systems feed the critical loads through a static uninterruptible ac power supply (UPS) subsystem (consisting of two battery chargers, a 120-cell lead-acid battery, and a 90-kVA three-phase static inverter). Thus, if the three primary power sources fail, the lead-acid battery is powerful enough to carry the critical loads for the center’s functions for at least three hours.

The IBM computers take action on the data collected from the control centers of NYPP’s eight member systems. Real-time processing permits the computer to maintain on-line status data on all generating facilities and transmission lines in the state. The information gathered and processed by the computer is put on the control room display board, the dispatchers’ four-color digital CRTs, four strip-chart recorders, two multipoint recorders, and four logging typers.

NYPP’s “baptism of fire”

The equipment at the Guilderland control center received its first major test during the afternoon of August 18, 1971, when the NYPP was afflicted by three almost simultaneous outages:

- The incidence of a line-to-ground fault by the sagging of a 345-kV transmission line onto a tall fir tree in Baldwinsville, N.Y.
- Loss of generation at a 500-MW generating station near Oswego, N.Y.
- Trouble on an Interconnection with the PJM power pool.

Fortunately, the NYPP weathered the crisis with a minimum of inconvenience: emergency power imports from New England, an automatic 8-percent voltage reduction in the Con Edison service area, and a brief cutoff of power to 200,000 customers of the Long Island Lighting Co.

Strengthening the power pool

A considerable amount of new generating capacity has been added to strengthen the CANUSE system since 1965; also, new transmission and tie lines have been built to “beef up” the reliability and efficiency of the total power pool. For example, Orange & Rockland Utilities, Inc., has two new large oil-fired generating plants on the west bank of the Hudson River at Roseton in Orange County, and at Bowline in Rockland County, and the large nuclear complex at Indian Point in Westchester County has added 3300 MW of generation.

In addition, from 1970 to 1973, Con Edison Installed more than 2000 MW of gas-turbine generation in New York City, both for peak-demand hours and as “insurance” against another system-wide blackout. According to NPCC, 500-kV transmission lines, increased from 650 km in 1965 to 1050 km by the end of last year; and the length of 345-kV transmission has quadrupled In the same ten-year period. Also, the 230-kV lines have increased from 9800 km to 12,500 km over that time span. Further, much of the increase in the 345-kV overhead and underground transmission has been Installed near and under New York City. Transmission lines on the eastern side of the Hudson River, down to New York City, have been upgraded, and new lines west of the Hudson have been constructed.

Over the past 11 years, stronger tie lines have been established with the neighboring PJM system (with its extensive 500-kV primary transmission network).
could hear ominous reports coming over pocket transistor radios: “The entire Northeast seaboard has lost power. The FBI and Department of Defense are investigating the possibility of widespread sabotage as a prelude to an enemy attack . . .” or “UFO’s may be responsible for disrupting the earth’s magnetic fields . . .” Admittedly shaken by some of the wild rumors being broadcast or whispered in anxious tones, we trudged homeward through throngs of pedestrians. The eerie ‘darkness was slashed only by the headlamps of motor vehicles. Meanwhile, civilians with flashlights were efficiently directing and ensuring an orderly traffic flow. Rooms at hotels en route up Fifth and Madison Avenues were rapidly being filled up by stranded commuters.

Dorothy Ellison, writing in the October 1975 issue of Con Edison’s house organ Around the System (in observation of the tenth anniversary), described the blackout:

“There wasn’t the slightest indication as to what was about to happen. November 9 was a crisp, clear autumn day. By late afternoon, conditions at Con Edison were typical for that time of year. The system had just passed its daily peak demand. Load was starting to drop off. Generators were, . . . producing 4550 MW of power.

“Another 220 MW of power was coming in over interconnections. . . to meet our load of 4770 MW. And there was a comfortable spinning reserve of 1350 MW available from company generators . . . The system was in good shape.

“And then it happened—the most massive power failure in history. At the height of the homebound rush hour, hundreds of thousands of people were trapped in crowded subway trains, elevators, unlighted halls and stairways. Planes heading for New York had to be diverted as far away as Bermuda as airports were plunged into darkness . . .” As far as New York City was concerned, the power “interruption” would last up to 13½ hours.

What’s to prevent another November 97

The ‘65 blackout triggered the most intensive investigation and analysis in the history of the power industry. As of the end of 1965, executives from the Northeast utilities began a reassessment of the entire philosophy of interconnections and of the institutional resources and procedures for coordinated planning and operations then being practiced. They arrived at a succinct conclusion: Although the interconnected network provides a high level of reliability to the consumer, it could be made more reliable by improved coordination in the planning of future power systems and in daily system operation. Such thinking led to the formation of groups like the Northeast Power Coordinating Council (NPCC) and the National Electric Reliability Council (NERC); see box, p. 84.

While maintaining reliability is still a primary concern of the regional councils, power pools have attempted to increase the efficiency of the large, integrated systems that comprise the regional networks. The New York Power Pool is a typical example (box, p. 85). It depends upon ‘a computerized power control center (PCC) to collect and analyze data from the pool’s eight-member power systems. Telemetered data are sent directly to the PCC, located near Albany, N.Y., from sensors installed on member companies’ equipment. Strip recorders at the PCC plot analog data such as system frequency, cumulative frequency deviation, and total load. Dispatchers receive an alarm whenever an analog signal exceeds upper or lower limits.

The PCC also collects bulk data that include real and reactive line loadings, breaker status indications, and the power generated by each unit or station. “Red flags” are displayed in two ways: on the dispatchers’ CRT screens or on a route board that displays all major transmission lines, substations, and generating stations in the pool. In the event of a contingency, the senior pool dispatcher may direct each member system within the PCC to pick up an appropriate share of reserve.

As a last resort to balance load with generation, the pool can order load reduction. The NPCC requires each system on its interconnection to provide facilities to relieve a minimum of 25 percent of its load automatically, as well as a means to relieve 50 percent of the load manually within ten minutes. Automatic underfrequency relays are set to shed 10 percent of load at 59.5 Hz or lower, and an additional 15 percent at 58.8 Hz. NPCC policy requires that, following a generation deficiency of up to 25 percent of the existing load, the frequency will return to at least 58.5 Hz in 10 seconds or less, and to at least 59.5 Hz in 30 seconds or less. If, at 58.5 Hz, the frequency is still declining, all systems are required to shed up to 25 percent of load manually and take whatever steps are necessary, including isolating units with local loads (“island forming”), to preserve generation and to minimize damage and service interruption.

Operating reserve policies are also in effect to provide reasonable protection against equipment failure. For example, each area within the NPCC provides a ten-minute reserve that must be at least one half spinning reserve (the portion of unused generating capacity that is synchronized to the system). This reserve must be sufficient to replace what is known as a “single contingency loss”—such as the forced outage of a generator.

Regional councils have also simulated the effect of “possible, but improbable,” contingencies on system performance—for example, the loss of all transmission circuits on a common right-of-way. The prevailing philosophy is one of “if the system survives definable contingencies, it can survive ‘oddball’ occurrences.”

In the area of hardware, protective relays have been upgraded, with minimum maintenance periods established for service beyond the initial break-in period. Redundancy is the byword: generator faults severe enough to disturb the bulk power system must be detected by more than one protective relay system; each area in a transmission station must be protected by two independent relay systems; and two independent relay systems are required on transmission lines.

Of course, no matter how many back-up relays are provided, the limits for line loadings are still set by humans, and exceeding those limits continues to be a cause of perhaps 10 percent of system disturbances. Eleven years ago, ignorance of the relay setting, in combination with a lack of load shedding, caused the blackout of November 9. Two years later, the PJM region suffered a blackout for similar reasons: no load shedding and a system that was operating out of limits (in spite of the fact that line loadings were posted on the wall).

Today, no power system in the world equals the proven reliability of the North American power grid and the probability of a widespread interruption in the Northeast, has been greatly reduced since the blackout of 1965. Yet the possibility of blackouts still remains.