Fail-safe power and environmental facilities for a large computer installation

by R. C. CHEEK
Westinghouse Electric Corporation
Pittsburgh, Pennsylvania

INTRODUCTION

For a modern large-scale computer installation, the reliability of the power supply and environmental conditioning systems is as important a consideration as the reliability of the computing equipment itself. This is especially true of installations which involve on-line real-time and time-sharing operations, in which no convenient re-start point is available for re-umption of operations after an outage. It is becoming more and more important in batch operations, many of which have grown in scale to the point where the expense of lost time due to re-starts can be a major economic factor.

Reliability of power supply, as the term will be used in this paper, refers not only to the continuity of power but also to its quality in terms of constancy of voltage and frequency and its freedom from momentary transients and surges. From the standpoint of general continuity, the typical electric utility power supply is excellent. However, this continuity is achieved by the provision on the power system of redundant lines and circuits equipped with fault-detecting relays, so that a line on which a fault occurs can be automatically and quickly removed from the system. Inevitably, the fault itself creates a transient voltage surge which is propagated generally over the system, and the switching operations required to isolate the faulty line create additional transients. These transient voltages often find their way into users circuits. They go relatively unnoticed by the average user, but they may induce a delicate flip-flop circuit in a computer to flip when it should flop and play havoc with a program in the process of being executed. As will be pointed out later in this paper, such transients may be transferred by induction between circuits which upon casual study appear to be completely isolated electrically as far as metallic connections are concerned. For example, they may appear in the output of a motor-generator set by induction due to the proximity of the generator output wiring to the motor input wiring.

The continuity of service required of environmental conditioning equipment is only slightly less critical than that required of electrical power. A failure or outage of a few seconds to a few minutes can usually be tolerated before performance of the computer system begins to be affected. This means that suitable temperature and humidity detectors can be used to sense trouble conditions and sound alarms in time to permit stand-by equipment to be manually switched into service and avert a computer shutdown. However, it is obviously better to plan the system in such a way that manual intervention is not necessary in case of failure of a particular component.

The provision of fail-safe electric power and reliable environmental conditioning for the computing facilities of the Westinghouse Tele-Computer Center was a matter of serious concern from the outset of the planning for the Center in 1961. The measures eventually taken to achieve these goals considerably exceed those initially thought to be adequate; so it is obvious that a few lessons were learned along the way. The purpose of this paper is to describe the evolution of these facilities; to recount some of the problems encountered and their solutions; and generally to share with others the benefits of some experience in this relatively neglected area of planning for computer systems which must provide a high degree of operating reliability.

It should not be inferred that the solutions described in this paper are the only suitable ones. Recent developments have placed a variety of approaches to these problems at the disposal of the planner of a new facility. In the evolution of the systems at the Center, the designs were based on the best available balance between economy and the degree of reliability desired, using the approaches available at the time.

Power supply facilities at the Westinghouse Tele-Computer Center

The Westinghouse Tele-Computer Center is the cor-
porate-level computing and data communications facility of the Westinghouse Electric Corporation. Operations began late in 1962 with a single UNIVAC 490 Real-Time System, initially performing teletype message switching on the Corporation's private teletype network, along with a variety of straightforward batch processing applications. The Center is located at a site in suburban Pittsburgh, where the only available utility power supply was a conventional 4160-volt radial distribution circuit, serving many small commercial establishments and residences in the vicinity. It was obvious at the outset that this circuit would not meet the needs of the Center, not only from the standpoint of reliability but even its ability to provide enough power under normal conditions to supply the projected load. It was therefore necessary to have power at 23-kv brought to the site by the utility from a 23-kv subtransmission circuit approximately a mile away which interconnected two of the utility's 23-kv substations. This would have provided adequate capacity, but considerations of reliability led to the decision to have a second 23-kv feeder brought into the site from a geographically separate 23-kv interconnection approximately three miles away. The two 23-kv feeders were built on separate pole-lines on each side of the road along which they run together for several hundred yards before entering the property, and they share common poles only after entering the site. It was also decided to install a private substation on the site, in order to incorporate in it special relaying and switching equipment for transfer of the load from one line to another in case of failure.

The substation (Figure 1) incorporated two identical 1500 kva transformers, 23 kv to 4160 volts regulated, either of which alone could supply adequate power for the whole building to the 4160-volt bus in the outdoor substation. The 750-kva power center inside the building, supplied from this bus, stepped the 4160 volt power down to 120/208 volts for distribution within the building. The power distribution unit for the UNIVAC 490 computer system was supplied by one feeder from this power center. It supplied power directly to blowers, motors, and other "non-critical" units in the computer system, as well as to a motor-generator set which in turn provided regulated voltage, presumably free of surges and transients due to external system disturbances, to the central processor, communications control units, and other units which were deemed to be critical in sensitivity to power fluctuations.

Both the "raw" power and the "regulated" power were distributed throughout the computer room in enclosed common wireways, separate from signal cabling which was laid in open cable trays.

The original scheme of operation was to supply the total power requirement of the site from one of the 23-kv lines with its associated transformer. The other transformer was kept energized by its 23-kv circuit, but its 4160-volt breaker to the bus was kept open. An undervoltage relay on the 4160-volt bus detected loss of voltage on the bus due to failure of voltage on the 23-kv circuit normally in use and transferred the load to the other transformer and line by sequentially opening the breaker from the faulty source and closing the breaker to the other. Relaying and circuit breaker operating times were adjustable to considerably less than a second, and it was felt that the inertia of the m-g set supplying the critical computer units would be sufficient to maintain adequate speed to keep these units supplied with power during this period. Also, it was felt that any fluctuations in frequency at the output of the generator would be gradual and therefore not disturb the operation of the system it supplied.

These assumptions were probably correct, and the theory of operation described was probably very good, as far as it went. However, during repeated tests of the transfer scheme during the remainder of the winter of early 1963, and upon the one or two occasions when power actually did fail and initiate a transfer, the transfer was never accomplished without resulting damage to the programs running in the UNIVAC 490 and an abrupt shutdown of the entire computer system. During this period more and more units of the computer system were moved to the isolated supply, on the theory that perhaps some of them which previously were deemed noncritical were actually injecting false inter-
rupts or other spurious signals into the central processor and affecting its operation. The transfer time was shortened to the minimum possible, less than half a second. However, these efforts were to no avail, and although the possibilities of this line of approach were exhausted, the transfer scheme was still unsuccessful.

But the worst was yet to come. With the advent of spring came the thunderstorm season, and it was quickly learned that when the skies began to darken with thunderclouds it was good tactics to get the recovery-program tapes out of the racks and ready to mount, because an outage was probably imminent. It was also found that even an instantaneous transfer scheme would not have solved the problems, because surges due to lightning strokes and resulting switching operations on remote parts of the utility’s power system of duration sufficient only to cause a momentary light flicker at the site, were enough to shut down the computer system.

It was then concluded that it was these transients in the “raw” power source, induced into the wiring of the presumably isolated power source due to their proximity in the common wireways, which were causing the trouble. Furthermore, it was apparent that no scheme for transferring to an alternate source of power would work under these conditions, because the switching transients set up by the transfer itself would defeat its major purpose.

A solution might have been to rewire the entire computer system, isolating the wiring for critical units in separate wireways and keeping it separate throughout all parts of the system. However, this would not only have been quite expensive but would have required extensive shutdowns of the system, which was not feasible at the time. It was decided to take a “brute-force” approach and supply the entire computer system with isolated power from a single large motor-generator set, with the output power leads from the generator well separated from the raw power source to the motor.

The motor-generator system selected is called the “constant-frequency” or “CF” system, in which a conventional m-g set is mechanically coupled to a high-speed flywheel through a controllable eddy current coupling or electrical clutch (Figure 2). Under normal conditions the motor receives power from the input line and drives the generator in the conventional way. The flywheel, disconnected from the system by the electrical clutch, is driven by a separate motor at a higher speed. Upon failure of normal power, which is sensed by voltage and frequency sensors on the input line, the clutch is energized under control of a frequency regulator at the output of the generator. The coupling of the flywheel to the m-g set is controlled in such a way that the flywheel gives up its energy to the system at a rate which maintains the speed and therefore the frequency and voltage of the generator until the flywheel slows down to the speed of the m-g set.

Such a system, rated at 80 kilowatts, with a flywheel sufficient to supply full output for a minimum of 12 seconds after loss of input power, was ordered for installation before the lightning season of 1964. Upon installation of this system, it was immediately possible to realize the planned benefits of the alternate power transfer scheme. Several failures of the normal power line subsequently occurred. Except for a momentary outage of the computer room lights (which were on a separate circuit from the computer system), computer operating personnel would have been unaware of the fact that transfer to an alternate power source had taken place, because the computer system was unaffected. Furthermore, during the lightning season of 1964 alone, this system averted many outages and the loss of information and time that would have resulted from the many power-line disturbances that were noted.

Although several failures of the normally-used power line have occurred each year, they have been of very short duration. And in every case but one, the alternate source was available, and the transfer was made automatically and successfully without interruption to the real-time operations. Fortunately the one case referred to, in which the alternate source failed simultaneously with the normal source, occurred during a weekend when real-time operations were already suspended.
The computing facilities of the Center have expanded tremendously from the single UNIVAC 490 system with which operations were begun. These facilities (Figure 3) now include dual UNIVAC 494 central processors in addition to the original 490, which is still in service; a dual CDC 6600 system with a 6416 scheduler and control processor; and an IBM 360/50-75 system in an ASP configuration. This concentration of processing power correctly suggests that the volume and variety of the applications handled by the Center have expanded greatly also, and it is no exaggeration to say that a prolonged loss of power could have very serious consequences to the operation of the entire Westinghouse Electric Corporation.

The construction of a second building at the Center during 1966 and 1967, larger than the first, required replanning of the power supply facilities. The lessons of the widely publicized Northeast power blackout led to a reappraisal of the initial policy of complete dependence upon the public utility supply for power. The decision was made to install a quick-starting diesel-engine-driven generator as an alternate supply. With each of the three major systems supplied by its own constant-frequency m-g set, capable of providing full power for 12 seconds after failure of the prime source, it is possible to sense the failure, start the engine and bring it up to full speed in 10 seconds, adequate time to pick up the load of all three systems without interruption. The engine-driven generator is rated at 800 kilowatts, sufficient to supply all the computer systems as well as the critical auxiliary items needed to maintain computer operations. These critical auxiliaries are listed in Table I.

An important factor to consider in planning a system using an engine-generator is the ability of the generator to supply the starting KVA requirement of any large motors which may be dropped during the outage. In the case of the CF units, because the motor-generator combination is kept at rated speed by the flywheel until the engine-generator is ready to provide power, there is a momentary transient lasting only a few cycles, while the motor adjusts itself to the supply frequency. The control system allows a short time delay for this to occur before re-connecting the chillers, air-handling units, and pumps to the 208-volt bus. The KVA capacity of the generator is adequate to start the chiller units, which are by far the largest motors on the system and the only ones which might present any problem.

In this system (Figure 4), the bus-tie breaker is normally open. Undervoltage relays detect loss of power on the portion of the 4160-volt bus normally used to supply the computer systems. If the other portion of the bus is still energized, the transformer breaker is opened, the bus-tie breaker is closed, and the other 23-kv source supplies power to the entire bus. Meanwhile, the same signal is used to energize the cranking system for the engine-generator. If power is not available from the other 23-kv source, the tie breaker remains open and the generator is connected to the 4160-volt bus as soon as it achieves rated speed and voltage, provided normal power has not returned in the interim. Once the engine-generator is connected to the bus, the system does not reverse itself automatically even though the normal supply is re-energized. The transfer back to normal power

### Table I—Westinghouse Tele-Computer Center Critical computer and auxiliary load

<table>
<thead>
<tr>
<th>Category</th>
<th>KVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Systems</td>
<td></td>
</tr>
<tr>
<td>UNIVAC 494 Systems (CF Set)</td>
<td>125</td>
</tr>
<tr>
<td>IBM ASP System (CF Set)</td>
<td>200</td>
</tr>
<tr>
<td>CDC 6600 System (CF Set)</td>
<td>200</td>
</tr>
<tr>
<td>Air Conditioning Compressors</td>
<td></td>
</tr>
<tr>
<td>IBM and CDC Chiller Compressor</td>
<td>160</td>
</tr>
<tr>
<td>UNIVAC Air Conditioning Compressors</td>
<td>40</td>
</tr>
<tr>
<td>Fans and Pumps</td>
<td></td>
</tr>
<tr>
<td>IBM Room Fans</td>
<td>30</td>
</tr>
<tr>
<td>CDC Room Fan and Pump</td>
<td>30</td>
</tr>
<tr>
<td>UNIVAC 494 Room Fans</td>
<td>15</td>
</tr>
<tr>
<td>Cooling Tower Auxiliaries</td>
<td></td>
</tr>
<tr>
<td>Pump</td>
<td>15</td>
</tr>
<tr>
<td>Diesel Heat Exchanger Pump</td>
<td>10</td>
</tr>
<tr>
<td>Chiller System</td>
<td></td>
</tr>
<tr>
<td>Electric Heater for Humidity Control</td>
<td>30</td>
</tr>
<tr>
<td>Lighting—All Critical Areas</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>995</strong></td>
</tr>
</tbody>
</table>
supply is performed manually. In this case again, the CF units provide a 12-second period during which the generator may be removed from the bus and the transformer breaker energized to restore normal supply from the main power transformer.

**Static inverter power supplies**

An alternative to the use of motor-generator sets for reliable power supply has been developed since the system described for the Center was designed. Rapidly increasing power capability and decreasing costs of power semiconductors have now made static inverter systems feasible as power supplies for large computer installations.

The basic elements of a typical inverter system are shown in Figure 5. The system consists essentially of a battery charger (static rectifier), a battery, and a static inverter. The rectifier converts input a-c power to d-c, maintaining the charge on the battery as it supplies d-c to the inverter, which converts the d-c back to a-c to supply the load. In case of failure of the input power, the battery supplies d-c to the inverter, maintaining the power to the load without interruption for a period depending upon the battery rating (several minutes in a typical installation).

In addition to providing a temporary source of power until alternative supply sources can be brought into service, the battery performs another important function. It acts at all times as a filter of almost infinite capacity to prevent power-line transients and surges from being transmitted through the system to the load.

Being completely static, the rectifier/battery/inverter system requires little maintenance and is clean and free of noise.

Such systems are now available with ratings from 1 kVA to 400 kVA, and several systems can be paralleled if necessary to achieve still higher total power capability.

Although the initial cost of a typical complete system is generally somewhat higher than that of a motor-generator set, the lower installation and maintenance costs and the operating advantages make the system an extremely attractive alternative.

**Air-conditioning systems**

In the planning of the air-conditioning system for the original 490 computer installation, it was concluded that a total of 20 tons of compressor capacity would be adequate to supply the units of the system which used room air for cooling. Certain critical units, including the central processor, were cooled by a separate ducted system, for which 20 tons of cooling also was sufficient. Each system had adequate cooling capacity for future expansion. Here again a stand-by system was designed, and the system finally selected used two 10-ton reciprocating units each for the room and the closed supply. For each system, an additional 10-ton unit was provided as a stand-by for each 20-ton combination. Air-to-air systems were used, partially to avoid the dependence upon continuous water supply that would have been inherent in a condensing-water system.

The controls were designed so that on each system, one 10-ton unit supplied the base cooling requirement, the additional compressor being cycled on and off under thermostatic control to supply the incremental cooling requirement. The system provided for manually-controlled substitution of the stand-by compressor for either of the normally-used compressors. Each of three compressors supplied its own separate set of cooling coils in the air ducts to the room system and the closed system respectively.

The initial control design provided for damping or modulation of the air flow by means of thermostatically
controlled vanes in the air ducts, so that control of temperature could be maintained within one degree despite the “on-off” cycling of the second compressor in each system. Since there was more than adequate cooling capacity provided when both compressors were on, the vanes cut down on air flow under this condition to maintain steady supply-air temperatures in the room and in the equipment.

The most important lesson learned from experience with this scheme was that a simple, reliable control system with a minimum of complication is far preferable to a complex, sophisticated one which theoretically provides more precise regulation. One of the requirements of a reciprocating compressor is that once it is started it should be run for some minimum period of time in order to insure proper lubrication (in this case a minimum time of four minutes). The control system was arranged so that once a compressor was started it automatically ran for this minimum time, even though there was no longer a cooling requirement for it. The result was that the air-flow modulation system occasionally closed the vanes in the ducts so far that ice formed on the cooling coils due to the restricted air flow. Once this began, the effect was cumulative, and it was not long before the cooling coils completely restricted air flow in the system. The result was a complete loss of air flow until all compressors had been shut down long enough to permit the ice to melt away.

The high-precision temperature control system was quickly abandoned, and the vanes in the air ducts were permanently propped wide open. The temperature was allowed to decrease as it would during the minimum cycle time of the cycling compressor on each system. Although this sometimes meant a variation of temperature in the ducts of as much as three or four degrees below the control temperature, this cured the icing problem and provided much more reliable operation. Another restriction involved in the use of an air-to-air system is that it is harmful to the compressor units to operate such a system when outside air temperature drops below a certain minimum figure, in this case 15 degrees Fahrenheit. The control system was arranged to shut down the compressors and use outside air directly for cooling when this outside temperature was reached. This involved another complicated system of controls and vanes to mix outside air with recirculated air to maintain proper temperatures, one with which adequately reliable results were never obtained.

In general, experience with the air-to-air system and reciprocating compressors was not good, and in the planning for expansion a chilled-water system was designed, using centrifugal compressors (chillers), which are theoretically much more reliable. This has proven to be the case. Before adopting this system, however, arrangements were made for water supply from alternate directions to the water input line to the site, with isolating valves on each side of the tap, so that a water-main break in either direction could be quickly isolated.

The system as it is now operating uses two 120-ton centrifugal chillers, providing chilled water to the water-to-air heat exchangers in the CDC-6600 and IBM computer rooms. The chillers in turn are supplied with condensing water circulated through outdoor cooling towers. Although the chillers are physically essentially in parallel, the control system operates the chillers in sequence. One chiller is sufficient to supply the entire cooling requirement of both computer rooms. The other is normally de-energized, and its condensing-water and chilled-water pumps are stopped. Thus, the first chiller takes the entire load. If, however, it should fail, or if any of its auxiliaries should fail, the resulting rise in chilled-water output temperature will cause the second chiller and its auxiliaries to be energized automatically, restoring normal cooling capacity without manual intervention.

Experience with this system has been very satisfactory. The centrifugal chillers are very quiet, reliable, and vibration-free. The water-to-water system presents no seasonal problems as does the air-to-air system. Because chilled-water supply temperature to the air-handling units in the computer rooms is a minimum of 45 degrees, there are no cooling-coil icing problems. Also, as described, the system provides its own back-up protection without manual switching.

SUMMARY AND CONCLUSIONS

1. For important computer installations, it is desirable to provide a back-up source of power which can be brought into service without interruption of continuous power to the computer system.
2. Unavoidable transients and surges on a utility power system can cause malfunction of a computer, and the power supply system should be designed so that these transients do not appear in the supply lines to the computer system.
3. Motor-generator sets with controlled-energy flywheels and rectifier/battery/inverter systems constitute two alternative means of isolating a computer system from transient voltages and maintaining continuous power while an alternative source is brought into service.
4. Simple environmental control systems with less precise regulation are preferable from the standpoint of reliability to more complicated systems with greater precision.
5. Operating experience at the Westinghouse Tele-Computer Center has proved chilled-water cooling systems with centrifugal compressors to be more reliable than air-to-air systems with reciprocating compressors, despite the requirement for essentially continuous water supply.