4. Transmitter Engineering and the 'Ilities'

Fear and loathing on the transmitter-design trail.

No discussion of high-power transmitter design would be complete without mention of the impact of the "ilities," of which the most familiar are

- Reliability,
- Maintainability,
- Availability,
- Electromagnetic susceptibility, and
- Electromagnetic compatibility.

In the same category, but not literally "ilities," are

- Safety,
- Built-in test equipment,
- Failure-mode and effects analysis,
- Human factors, and
- Configuration control.

In the full realization that entire books have been written on each of the above subjects—and that the subjects themselves produce fear and loathing in most red-blooded design engineers—the author shall nevertheless hazard a few comments.

4.1 Reliability

Most engineers, especially those who have worked on military contracts, are familiar with, or at least have heard of, MIL-HDBK 217, the so-called reliability bible. Pentagon officials would like to think that an engineer with MIL-HDBK 217 in one hand and an electronics parts list in the other should be able to calculate any electronic system's reliability in terms of the mean time between failure (MTBF). Except for certain parallel-redundant, fault-tolerant special circuits, the military assumes that the failure of a single component should result in the failure of the circuit to perform properly. (After all, if the circuit performs properly without the component, it wasn't needed in the first place, right?) In which case, the total failure rate of the circuit is the sum of the failure rates of the individual components. These individual failure rates can be found in MIL-HDBK 217. The MTBF is the reciprocal of the total failure rate, except for one thing. The failure rates in the handbook are *random* failure rates. These are the rates that apply throughout the flat bottom of the so-called bathtub-shaped curve that describes the useful life of a component. The downward slope at the beginning of the bathtub is due to "infant mortality" of the less robust components, and the tilt up at the other end is indicative of the "end-of-life syndrome." Unfortunately, these statistical preconceptions do not always apply to transmitters.

In the first place, for high-power transmitters few components have the luxury of random failure. Systematic and catastrophic failures are more the rule than the exception. Stress levels have many more dimensions than those that can be encompassed by a reliability handbook. For instance, take the case of a conventional wire-wound resistor performing the function of current-limiting resistance described earlier in Chapter 2, Section 6. This resistor will have average-power dissipation because the flow of pulse current through it is on a repetitive basis. Its thermal properties and/or external cooling must be adequate to limit its average temperature. But there are other considerations. There will be pulse heating in the resistor because the current flowing though it is in the form of pulses. Worse yet, if there is a high-voltage arc in the system downstream of the resistor, perhaps all of the energy stored in the system will be dissipated in the resistor in so short a time that heat will not be able to leave it. In addition, all of the system voltage will be applied across the resistor. And that is not the end of it. The fault current (which, indeed, the resistor is intended to limit) may be 50 to 100 times as great as the normal pulse current. Finally, magnetic pressure, which is proportional to the square of this current, will attempt to unravel the resistor, and this force is by no means negligible. In fact, all components in the high-voltage/high-current path are subjected to similar sets of layered stresses.

Even low-level components, which seemingly should be farther out of harm's way, can be subjected to induced, convected, and conducted impulse stresses that can produce instantaneous mortality or, sometimes even worse, weakened or altered states. In modern transmitter designs (except those designed by the Russians), low-level active components are exclusively solid-state. Easily 10% of the total component count in a well-thought-out design can be devoted to circuit elements whose purpose is to protect prime-mission components from damage or upset. Especially susceptible to damage are an integrated circuit's gate inputs, which must be current-limited and diode-clamped for survival. If you think that using solid-state devices with large-area junctions will eliminate the problem, think again. Solid-state junctions having a large surface area do not, in themselves, assure survivability, especially when subjected to short-duration overvoltages. Solid-state junctions fail because they are short-circuited by the growth of metallic lattices from one side of the junction to the other, a process as inexorable as the loss of emissive material from a thermionic cathode. As mentioned earlier, the rate of this chemical reaction is governed by the Arhenius equation, which states that the rate is a log-normal function of temperature. (This is why the failure-rate data given in MIL-HDBK 217 is for solid-state junctions whose temperature remains *below* 175°C.)

Solid-state junctions do not last forever. When they are subjected to short-duration overvoltage, current does not have time to spread out over the full surface area of the junction, nor does heat have time to be conducted away. An extremely high temperature, therefore, may be confined to a very small region of the total junction. The effect of this condition would be analogous to a large number of small junctions wired in parallel; the failure of one is all that is required for device failure.

There are subordinate attributes of devices that can be vehicles of failure as well. The power MOSFET, a relatively high-voltage, high-current switch that is used in many of the low-level transmitter circuits, has a residual bipolar transistor that manifests itself as an anti-parallel diode. Voltage reversal caused by abnormal external circuit conditions will produce current flow in this diode. If the flow is too much or too fast, the diode will fail, and the source-drain connections will be short-circuited. All solid-state diodes, after conducting in the forward direction, will conduct in the reverse direction even more vigorously until the charge has been removed. If this current is not limited, even "fast-recovery" diodes can be destroyed. (Later, we will describe two solid-state diode applications that had to be retrofitted in every sense of the word with thermionic, or "real," diodes because of the reverse-conduction effect—and ironically they had to be retro-designed *back* to solid-state devices because it was discovered that nobody manufactures high-voltage thermionic diodes any more!)

Multilayered stress affects almost all electronic components. That is why it is not really practical to rely on such guidebooks as MIL-HDBK 217, which only recount single-point failure rates and tell nothing about systematic or catastrophic failure rates. Designers must take into account the complicated array of potential stresses present in the system.

4.2 Maintainability

If the prospects for designing the perfectly reliable transmitter are bleak, it would be a good idea to devote some engineering attention to the maintainability of a transmitter. Fortunately, this is easier to do: design the transmitter so that all its components can be easily and quickly accessed for repair and troubleshooting.

One tenet of Murphy's Law states that the component most likely to fail is the one that is least accessible. (An as-yet-unproven corollary states that if all components are equally accessible, none will fail.) There are only two guidelines for designing transmitters with good maintainability:

1. Never mount a component on another component; and

2. Never mount a component or subassembly in such a place that you have to remove another one to get to it.

Needless to say, these guidelines are violated all of the time, and for perfectly justifiable reasons. But designers should at least be aware that they are violating a guideline. (A frequently encountered barrier to maintainability is the hardware used to affix covers and access plates. Every screw should be justified. If they are all needed for structural reasons or to keep wanted things in and unwanted things out, the fasteners had better be captive. If they aren't, you can bet that they will never be completely replaced once they have been removed.)

4.3 Availability

Availability is the bottom-line combination of reliability and maintainability. In most cases, it is what really matters to a user or customer. For instance, if a transmitter fails once per year on average and takes eight hours to repair on average, it is unavailable for service eight out of every 10,000 hours (roughly). Which means that it is available 9992 hours out of 10,000 hours, or 99.92% of the time. (This same availability could be achieved if the transmitter failed more frequently but could be repaired more rapidly.) Designing for maximum reliability is laudable and sometimes mandated, but is not always cost-effective or even affordable. Designing for ease and speed of maintenance is always cost-effective, especially if your reliability-enhancement efforts have done nothing more than identify those components that are most likely to fail.

Among the most costly transmitter designs are those with "100% availability." These are the parallel-redundant, multi-channel transmitters that possess something described as "graceful degradation." They have 100% availability, but at something less than 100% of maximum capability. All high-power transmitters with solid-state RF power amplifiers fall into this category, simply because it is not possible to achieve high power from solid-state sources except by the parallel combination of large numbers of individual modules.

But multiple-channel transmitters using microwave vacuum-tube power amplifiers have also been designed. The two biggest, the PARCS (Perimeter Acquisition Radar Characterization System), and the Cobra Dane radar, use multiple high-power TWTs and are phased-array systems. The PARCS uses 128 Raytheon PPA-200 UHF TWTs configured as 16 redundant eight-tube transmitters. The Cobra Dane transmitter uses 96 Raytheon L-band TWTs configured as 12 redundant eight-tube transmitters. The outputs of the TWTs are combined in space, as each tube feeds multiple antenna elements through phase-shifting devices. The loss of a single tube reduces the radiated power to $(N-1)/N$, but reduces the far-field power density to $(N-1)^2/N^2$. (This calculation takes into account not only the lost power but the lost antenna aperture as well.) In a transmitter such as the ALTAIR UHF transmitter, which combines the outputs of three PARCS-type eight-TWT transmitter subsystems into a single-waveguide antenna feed line, the loss of a single TWT reduces output to $(23/24)^2$ of the maximum total. An amount equal to 1/24 of the total is, obviously, the direct loss due to the defunct tube. A less obvious amount equal to almost another 1/24 results from an amplitude imbalance component of waster-load power throughout the power combiner matrix. Transmitters of this type degrade gracefully, but not quite as gracefully as their most ardent proponents would have us believe.

4.4 Electromagnetic susceptibility

How susceptible are transmitter circuits to upset or even destruction resulting from self-generated or external electromagnetic events? A designer may have no way of knowing until it's too late. The most tragic example of the effects of electromagnetic susceptibility was the fly-by-wire military helicopter, which lost its computer-generated control when it flew too close to certain radar systems and crashed (both figuratively and literally). All electronic circuits—digital, analog, or RF—are susceptible to external RF interference if it is at a sufficient power level and at an offensive frequency. For instance, there are few computers or word processors on the small Pacific island of Roi-Namur that can ignore the ALTAIR 7-MW, 162-MHz VHF transmitter when its 150-ft-diameter dish is aimed at the horizon and pointed in their direction. This is because transistor-transistor logic (TTL) circuits in the equipment depend upon the very small difference between the collector-saturation voltage of one transistor and the base-emitter turn-on voltage of the succeeding one to differentiate between a logical 0 and logical 1. The noise immunity designed into these circuits is virtually nil. Modern computer circuits are also fast enough to respond directly to bipolar-induced VHF signals. Hence, there is a guaranteed instant upset.

Yet the timing synchronization circuits for the ALTAIR, which share the same building as the transmitter, are oblivious to the same radiation. Still, they use integrated circuits that are functionally similar to the ones on Roi-Namur. What makes them different is that successive transistors are Zener-diode coupled. This feature introduces noise immunity equal to the Zener diode voltage. It also makes their gate response slower, but it is still more than fast enough for their dedicated purpose. The family of logic elements used for ALTAIR is Motorola's MHTL (Motorola high-threshold logic), which is only available for replacement purposes and is not recommended for new circuit designs. Teledyne makes a similar family called HINIL (high noise-immunity logic), and it serves the same purpose. (Members of this family have found their way into the antenna-servo logic of the same radar and for the same reason.)

In short, do not underestimate the impact of electromagnetic susceptibility on your design. As a minimum, designs *must* tolerate the radiation from the RF power source they are intended to serve. (It's also a good idea, as it certainly was on the island of Roi-Namur, to know who your neighbors are.)

4.5 Electromagnetic compatibility

The mirror-image of electromagnetic susceptibility is electromagnetic compatibility. To what extent will one piece of equipment intrude on another? When requirements for electromagnetic compatibility are expressly specified, they usually apply to so-called spurious or harmonic emanations, those that are superfluous to the prime mission of the equipment but that can be quite troublesome to adjacent equipment. For example, on the island of Roi-Namur there are high-power radar systems at VHF, UHF, L-band, S-band, C-band, K_A-band, and W-band—all but the last two of which are in the megawatt or multi-megawatt class. Not only must all of the transmitters—except the last two—meet stringent harmonic-suppression specifications, but the fundamental operating frequencies and band edges must be coordinated so that the harmonics of one do not coincide with or intrude into the operating band of another.

But the real issue here is interference. Put as simply as possible, if a system has excessive electromagnetic susceptibility, the designer had better head back to the drawing board, because even a superb job of engineering compatibility on the part of a transmitter's electromagnetic neighbors will not make that transmitter immune to their fundamental-frequency emissions. (It is worthy of note, however, that in some extremely crowded electromagnetic environments, fundamental-frequency modulation envelopes have been mandated. One of the most difficult to synthesize, but least sideband-intrusive, is the Gaussian envelope, which has the unique property of having identical shapes in both the time and frequency domains).

4.6 Safety

There are those who insist that designing a transmitter for safety is almost as important as designing it for its primary performance goals. They are wrong. It

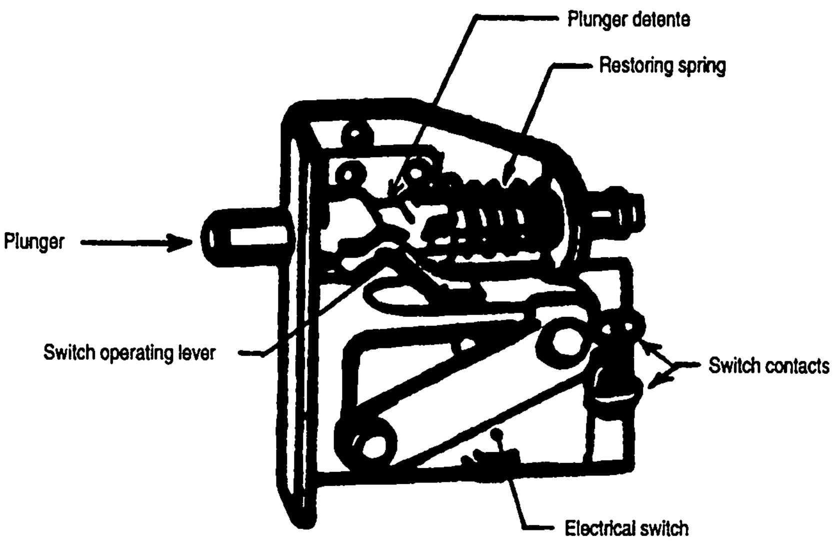

Figure 4-1. An example of a mechanically "cheatable" interlock switch.

is *more* important.

It goes without saying that all microwave vacuum-tube transmitters require operating voltages that can cause severe injury or death to a person who comes into contact with them. How high do these voltages have to be? Military specifications mandate that anything over 30 V be considered hazardous (which means that even all-solid-state transmitters are not exempt from safety-design considerations).

Exposure to hazardous voltages must be prevented by enclosing their sources. Access panels or doors to these areas must be interlocked in such a way that opening them automatically removes the hazardous voltage *and* short-circuits any circuit element capable of storing a charge or energy, even after the source has been interrupted. Electrical interlock switches are made especially for this purpose. Some have mechanical means whereby they may be "cheated" so that internal electrical power can be restored even with the access door or panel open. An example of a commonly used door switch is shown in Fig. 4-1. Note that the switch is normally actuated when the plunger is pushed in, as when a door or panel is closed or a lid is let down. When the door is opened, the spring deactivates the switch, thus opening the circuit. However, if the plunger is pulled farther forward by an impatient technician, the detent is overridden in the opposite direction and the switch is once again actuated. Unfortunately, this type of interlock is often used unwisely (or perhaps even illegally in this day of product liability). Where voltages are above 300 V, military standards forbid the use of "cheatable" interlock switches. (It goes almost without saying that any form of interlock system can be "cheated" if a technician has an adequate supply of time, tools, jumper wire, and nerve.) This complaint refers only to the type of switch shown in Fig. 4-1, which can be easily defeated by an unassisted individual. An especially robust form of "uncheatable" interlock is a mating male/female connector pair, as illustrated in Fig. 4-2.

What is important in designing for safety? It is *obvious* simplicity; it is defi-

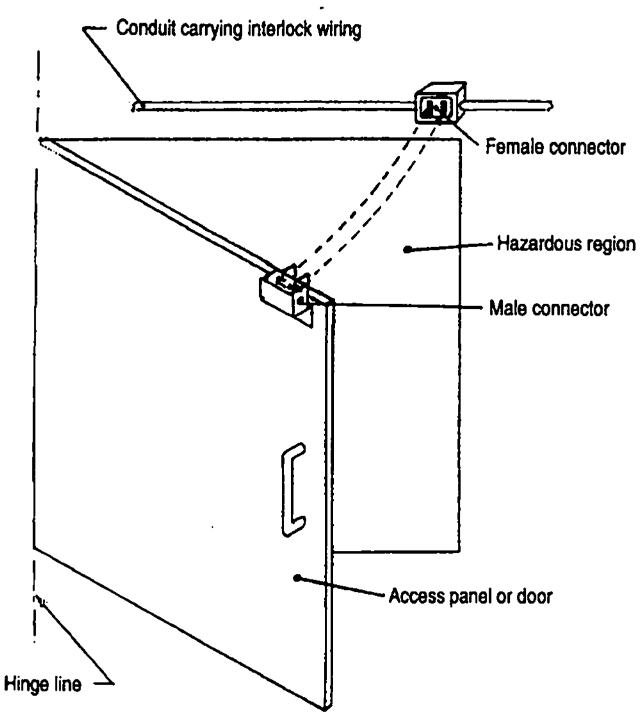

Figure 4-2. An absurdly simple, but surprisingly effective, non-cheatable interlock.

nitely *not* sophistication. When workers breach an interlocked enclosure, it is critical for them to know right away that the electrical de-energizing function of the interlock is working. An example of such a no-nonsense interlock can be seen in Fig. 4-2. In this switch, the continuity of the electrical circuit requires that the male connector, whose pins are jumpered together, be inserted in the female connector, one of whose terminals is connected to the power source while the other is connected to the load. The male connector is attached to the door, the female to the door frame. When the door is opened, the male jumper is pulled out of the female connector, thus opening the circuit. The status of the switch, and therefore the circuit, is immediately obvious to the person opening the door. This is a good interlock.

On the other hand, had the switch shown in Fig. 4-1 been used, the technician would never really know for sure if the interlock was working. In this case, the opening of the door removed the pressure that had kept an electrical switch in the closed position. The fact that the mechanical actuator of the switch had changed position may be obvious to the worker, but it would be by no means obvious that the electrical circuit has been broken. The key word is obvious. For interlock switches, the more obvious, the better.

The opening of an electrical-interlock circuit must also positively remove the hazard. Examples of such action are open-circuiting the hazardous-voltage conductors at the source end or short-circuiting the hazardous-voltage conductors at the load end. Preferably both should occur, in the order stated. One typical high-voltage shorting electro-mechanical relay is shown in Fig. 4-3. It is normally in the short-circuit position as shown; its solenoid electromagnet must be energized in order for it to hold its shorting bar in the raised position. If for any reason power is interrupted to the switch, the circuit is automatically shorted. It is, therefore, at least electrically fail-safe. A good designer would typically install such a relay in parallel with the transmitter's electronic crowbar (see Fig. 2-1, item 6).

Open-circuiting the hazardous voltage conductors at the source end can be accomplished with a series-opening switch. Figure 2-1 indicates two possible locations for it: the main circuit breaker of the unit substation (13) and the high-speed contactor (12). A favorite ploy of many safety-oriented designers is to make this switch the main circuit breaker, as long as it has an undervoltage trip feature. This feature, which is a field-installable option in some of the larger frame sizes, is often confused with the shunt-trip feature. It is the latter's logical complement. Whereas the shunt trip requires the presence of an external voltage to cause the breaker to trip, the undervoltage trip requires the presence of an externally supplied voltage in order to stay closed. Should this voltage be removed (or fall below a predetermined threshold), the breaker will automatically trip, and it cannot be reclosed until the external voltage has been reapplied. This feature makes it compatible with a fail- and connectivity-safe interlock topology and is highly recommended.

Before moving on to key-based interlocks, one more thing needs to be said about electronic crowbars. Although a crowbar can never be a proper component of a safety-interlock system, it has demonstrated more than once its capability to be a genuine life-saver—but only as the microsecond-response component

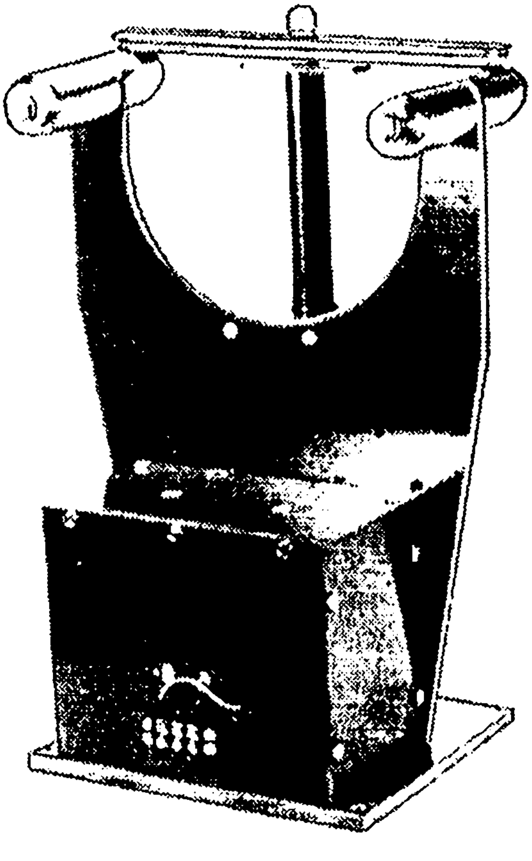

Figure 4-3. A typical high-voltage, electrically operated shorting relay.

of a ground-fault-interrupt (GFI) system involving the design of the entire high-voltage circuit. Harking back to Chapter 2, Section 10, where the high-voltage circuit was likened to household electrical service—with black (high-voltage), white (load-current return) and green (safety ground) conductors—Fig. 4-4 shows how this can apply to personnel lifesaving in exactly the same fashion as a bathroom GFI circuit. In the figure, the load on the high-voltage system is a microwave vacuum tube with an insulated (or isolated) beam collector. The rest of the tube envelope is metal and is fastened to ground, which establishes the single-point ground for the system. Both terminals of the high-voltage power supply and energy-storage capacitor are insulated from ground (black and white wires).

All current that flows in ground must also flow through the current-monitor transformer, which surrounds the single conductor that connects the low-voltage return conductor from the power supply to ground at or near the tube envelope. Assuming that the electron beam of the tube is well focused, about 99% of the beam current will flow directly between cathode and collector (dashed line) and only 1% will be intercepted by the ground part of the tube, called the body. Therefore, the normal current through the current monitor, even for a very high-power tube, may be less than one ampere. The threshold for the low-level firing circuit for the electronic crowbar, then, can be set for something only slightly greater.

The stage has now been set for our hero, who, standing on ground, has come in contact with the power supply high-voltage lead. Current through his (or her)

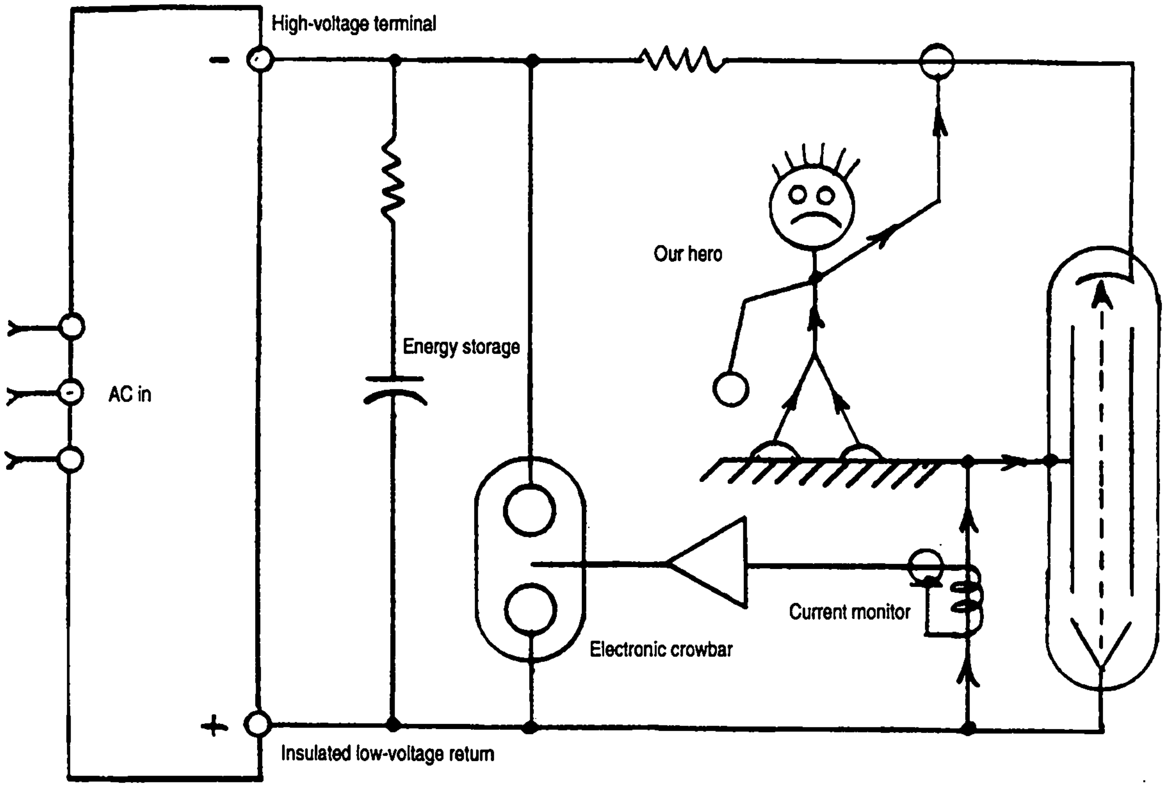

Figure 4-4. The electronic crowbar as a safety ground-fault interrupter.

body is treated no differently than microwave tube body current, and as soon as it exceeds the crowbar threshold, the crowbar will fire, diverting the lethal charge from our hero within microseconds. Actual lives have been saved in this way. (It is worth remembering that the French term for tube body current is I_{corpse}.) In order to be fully effective, however, the majority of the total current in the high-voltage loop must flow in a current path that does not include ground.

Automatic electrical interlocking is sometimes augmented by a key-operated system, the most common one being the "Kirk" key system, which can become quite elaborate. A typical system might involve a master key-operated switch, which shuts down power to a console or locks out a manually operated power-disconnect switch by extending a bolt. (The mating pieces of the system are pin-keyed so that the bolt cannot be extended unless the subassembly that includes the bolt is engaged with the piece that receives the bolt to effect the lockout.) Once the lockout has been accomplished, the key can be removed from the lock. (Until then, the key is trapped in the lock and cannot be removed.) The key, once removed, can now be used in a complementary subassembly to withdraw a bolt that may, for instance, have been preventing the opening of the door to a hazardous region. So long as this door is open, the key is again trapped, and can only be removed when the door has been closed and the bolt extended by rotating the key in the lock.

If there are multiple areas that may require simultaneous access, a component called a key-transfer assembly can be used. In theory, any number of keys can be trapped in such an assembly. A key can be freed only when the single access key is inserted in the proper lock and rotated. This procedure, in turn, traps the access key in the lock. Any or all of the subordinate keys may then be removed. These subordinate keys can be used to unlock as many areas as there are keys. The master access key, however, cannot be removed from the transfer block until *all* of the subordinate keys have been returned to their places in the block.

In order to assure safety, all of the keys must be coordinated and no duplicates can be tolerated (even in another system). It should be obvious by now, however, that the loss or misplacement of a single key would mean that the system could not be turned on. For this reason, the operators of most high-priority systems—and what high-power RF system would not consider itself high-priority?—have managed, one way or another, to obtain duplicate keys. (They insist the keys are kept in a "secure" place and under tight administrative control. Nevertheless, the entire safeguard philosophy of the system is subverted by this act.)

The hazards of high-power, high-voltage systems do not end with the possibility of electrocution, however. Stored electrical energy can be released with explosive mechanical force in the form of shattered solid-dielectric insulating bushings, the shards of which can have the same lethality as shrapnel. It has been calculated that one megajoule of stored electrical energy has the same explosive potential as half a pound of TNT. There is no reason to doubt this. The best enclosure for a large capacitor bank should act as both a shielded room and a blast vault.

Workers on high-voltage systems have also been known to drown or be asphyxiated as well. Systems operating at voltages much above 50 kV are often insulated with dielectric oil that is either petroleum- or silicone-based. These oils are less dense than water and often fill containment vessels that rival small swimming pools in volume. Therefore, they take considerable time to drain and refill. It is tempting to minimize repair or maintenance time by entering the tank without draining the oil. *Some* people have negative buoyancy in water. *Everyone* has negative buoyancy in oil. And a few have drowned because of it. Sulfur hexafluoride (SF_6) is also frequently used as a dielectric fluid. It is a colorless, odorless gas that is heavier than air, and it can fill a tank in exactly the same fashion as oil, displacing all of the air that originally filled the tank. If the tank is large enough for someone to enter it and become totally immersed in the SF_6, he or she can become asphyxiated without any warning from the body's defense mechanisms. At least one such death has been attributed to this cause. Large volumes of SF_6 are difficult, if not impossible, to make safe. They should simply be avoided in the design stage, if at all possible.

There are also two physiological hazards from RF radiation: the "microwave-oven" (or "English-muffin") effect and the acoustic-shock effect. The microwave-oven effect is the best known and understood. It involves the heating of internal organs and tissues when flesh and blood are exposed to microwave radiation. The acoustic-shock effect is caused by the kinetic energy contained in sonic waves that can emanate from the transmitter. These waves are especially hazardous to eyes, but the effect is only present in pulse-modulated RF systems.

High-power microwave-tube systems also operate at voltages high enough to generate ionizing radiation in the form of x-rays, which must be dealt with (usually in the form of added shielding). The latest, and most controversial, of the possible electrical hazards is extremely low-frequency (ELF) magnetic fields (in the milligauss range). Included in the range of suspect frequencies are the most popular power-line frequencies, 50 and 60 Hz, and some popular radar-system pulse-repetition rates, the most common of which is 30 pulses per second (pps). Exposure to high-current, high-voltage ELF has been linked in some studies to the development of leukemia in children. It would behoove the circumspect transmitter designer to stay abreast of the scientific and popular literature concerning ELF magnetic fields.

For better or worse, safety and safe design practices are increasingly becoming institutionalized. Environment, safety, and health organizations are becoming more pervasive and influential in government and private industry, gaining the administrative power to shut down systems that violate safety regulations. In the future, no high-power system design will be considered adequate unless it treats safety with the same, or greater, concern as its prime mission objectives.

4.7 Built-in test equipment

Just to insure its own proper functioning, any adequately designed high-power transmitter monitor and control system will inherently contain more test-point sampling points than most external users of such data are prepared to handle. If this is not the case, it is probably time to review the efficacy of the control and monitor system. (Later, as specific designs are discussed, the role of built-in test equipment will become clearer.)

4.8 Failure modes and effects analysis

In any high-power engineering project, the analysis of failure modes and their effects is a serious matter. The failure of a key component to function properly can initiate a true "domino" effect, leading to extensive subordinate (or collateral) component failure—or even to the electronic equivalent of meltdown. A memorable example of this took place at Dallas-based Continental Electronics during the testing of a 1-MW broadcast-band transmitter built for the Saudi Arabian government. The giant tetrode output tubes were protected from internal arc damage by an electronic crowbar in the form of an ignitron. When it fired for the first time, short-circuiting the entire high-voltage system preceding it, the special-purpose high-speed primary switch gear that was designed to disconnect the faulted high-voltage system from the primary ac mains not only did *not* respond with the intended speed, it did not respond at all! The faulted high-voltage system thus remained connected to East Dallas Power and Light. All the lights in the building dimmed until the valiant ignitron had been reduced to molten copper and a puddle of mercury. The high-voltage transformer/rectifier survived, thanks to a conservative design. What could have been a disaster resulted mostly in a spectacular short-term power bill. (Later it was discovered that a well-intentioned but not-so-well-informed technician found some "loose" hardware in the switch gear and tightened it down, thus preventing it from actuating properly.)

This little anecdote represents a good-news, bad-news story for Continental Electronics' failure-mode analysis. The good news was that the system's major components were designed to be robust enough to endure such an insult and suffer little or no damage. The bad news was that somebody forgot to predict the domino effect if the primary switch gear failed.

4.9 Human factors

Since 1949 the term for human engineering has been "ergonomics," which, as Webster's Ninth New Collegiate Dictionary states, is "an applied science concerned with the characteristics of people that need to be considered in designing and arranging things that they use in order that people and things will interact most effectively and safely." In this field, there are specialists who often have great awareness of the capabilities and limitations of humans in their interaction with machines. However, a properly designed transmitter, as will be discussed later under the subject of control and monitor, will act autonomously with electronic speed in order to safeguard itself from hazardous conditions. In some situations, there simply isn't time for human intervention. On the other hand, the control screen or control-panel displays, which alert the human operator as to what has automatically transpired and the reasons for it, must tell the story unambiguously.

Except for the most recent of transmitter control-system designs, such communication usually takes the form of indicator lamps that in the simplest case were either illuminated to show a function was enabled or off to show that it wasn't. The obvious source of ambiguity in this case is the burned-out lamp. More sophisticated designs used multicolored lamps: green for OK; red for fault; amber for standby. But even this system was not unambiguous. Some designers insisted that the turn-on of high-voltage should be indicated by a red light to denote that equipment has been energized, even though no fault is present. In such schemes, the potential for ambiguity is obvious.

The most recent designs take advantage of industrial-strength programmable-logic controllers (PLCs) and the almost-limitless multicolored, alphanumeric video display capabilities they possess. Far from simplifying the ergonomics, however, they make it all but mandatory that the user participate in the display design, or that a human-factors specialist be consulted to preclude a glut of uninterpretable data. PLCs now pose a real threat of converting more data into less information. It is the unambiguous and instantaneous information transfer between machine and human that is half of the goal of good ergonomic design. The other half—not surprisingly—is the optimization of the interface in the other direction: how unambiguous will the response of the machine be to a control input from the human operator? (Or, more correctly, how unambiguous will the operator's expectation be of the machine's response to a given control input?) As an example of this issue, consider for a moment the placement and shape of the accelerator and brake pedals in an automobile. These controls are so crucial to safe and effective operation that, once their shapes and positions had been established, they have never changed, while almost every other automobile control and indicator has been fiddled with in the interest of ergonomics.

4.10 Configuration control

The intention of configuration control, or configuration management as it is also called, is to make sure that a product, as it is routinely maintained or as parts are replaced following failure, remains the same as it was when it was first built. Unfortunately, in the case of a high-power transmitter, this is a virtual impossibility.

The reason for this, which will become increasingly clear as we move into specific designs, is that components, especially high-power components, simply are not being built any more in the quantity and diversity that they once were. Even low-level components, particularly special-function integrated circuits, obsolesce—or at least fall from favor. Therefore, they are no longer manufactured. (As a case in point, Motorola's entire line of high-noise-immunity gate circuits, which were used in many transmitter solid-state control systems, is no longer manufactured and has been relegated to virtual antiquity.) So, although configuration control is an admirable goal and high on many customer's and user's wish lists, for high-power transmitters the recent history of electronic component suppliers makes it just that: a wish.

How could such a situation have evolved? Can't the government, one of the biggest users of such electrical components, insist that replacement parts remain available? The answer is yes—to an extent. The problem for the high-power microwave transmitter field is that the government hasn't gone far enough. The system put in place to ensure that critical components would remain available, the joint Army-Navy (JAN) and military (MIL) standard categories of parts, has not identified enough components to populate even the simplest of transmitters. Therefore, transmitters tend to have a preponderance of non-standard parts, from a MIL-specification point of view. This means that the purchase of such parts must be justified through a Non-Standard Parts Approval Request and approved by the government-agency customer.

Compounding the overall problem is the fact that even though there may be perfectly useful standard parts in the JAN and MIL category that are generic in nature and ideally available from more than one supplier, there may not be, at any given time, a vendor qualified to produce them. There might not even be a vendor interested in manufacturing them!