EMP Defensive Strategies

Strategies that 'harden' electrical and electronic systems against electromagnetic pulses may save lives during a nuclear war and permit the restoration of society afterward

BY JANET RALOFF

The second of two parts

If the detonation of a high-yield nuclear weapon in the United States' upper atmosphere showered the nation with an electromagnetic pulse (EMP), how would American technology stand up? It's a question that can't be answered with any certainty today because the electronics revolution in the computerization of America is introducing an increasing EMP vulnerability to all segments of society. And that worries a multitude of defense planners.

EMP is a powerful and potentially devastating form of electromagnetic "fallout" associated with nuclear weapons (SN: 5/9/81, p. 300) and other major explosive bursts. Unlike radioactive fallout, this rain is believed harmless to living things but potentially lethal to electronics and electrical systems. It wreaks its havoc by inducing staggeringly large and rapid current or voltage surges through electrically conducting materials. And because nuclear weapons generate the most virulent form, it's not surprising that study of the phenomenon was cloaked in secrecy until the mid 1960s.

During the early 1960s, "it was so classified that if you said EMP out loud," jokes James Kerr, "you probably had to have your mouth washed out with secret lotion." Kerr, who is staff director for the Federal Emergency Management Agency's Technological Hazards Mitigation Division, said he was unable to study the effects of EMP on civil systems for his agency's federal predecessor in 1965 "because it was so classified." His goal had been the development of a guide for the protection of civilian systems and industrial facilities against wartime EMP. Kerr's guide eventually made its debut, eight years later.

What has been its impact? According to Mike King, an EMP-shielding analyst who until last July worked at the Defense Nuclear Agency in Washington, "I think, basically, that civilian industry per se has totally no regard for EMP. I guess their theory is, 'Hell, if we're going to be under a nuclear attack, why am I worried about my computer file?' " SCIENCE NEWS confirmed in interviews with several industrialists that that view is one being used to justify ignoring the hardening — or protection — of equipment against EMP within the electric power industry.

In a paper issued last December, FEMA's Russell Clanahan attempts to counter such attitudes. "Much of the destructiveness of a nuclear attack, in lives and property lost, depends on the unpreparedness of the one attacked. In a sense, ... the unwillingness to confront the situation and prepare becomes a self-fulfilling prophecy."

Perhaps if EMP protection were relatively inexpensive, there would be less resistance to hardening. But there is "a pretty impressive price tag" associated with hardening, notes Bill Macklin of IRT Corp. (a firm that has specialized in EMP work for the military). Estimates vary, but it could cost at least an extra 15 to 20 percent to build EMP protection into a new facility. And the higher cost would go not so much for added or more expensive equipment, explains Ralph Sinnott, an electronics engineer with FEMA, as for "seeing that tradesmen do the construction differently." EMP-hardening an existing facility can be notably more expensive.

Perhaps the largest controversy in EMP-hardening — one Macklin describes as being almost "theological" in nature — has developed in response to the tackling of these potentially expensive retrofit cases. At issue is whether to shield all vulnerable components in a metal box, generically known as a Faraday cage, or whether to seek out and selectively shield only the most vulnerable components.

It may not sound like a big deal, but Macklin says that while the latter, tailored approach could involve more design analysis, it could also cost "almost an order of magnitude less" than installing a Faraday cage. That becomes an attractive selling point when the economy is undergoing a fiscal belt-tightening. In addition, tailoring in smaller, selective changes to an existing system usually proves less disruptive to its users — for example, no workers tearing out existing walls, ceilings or floors — during the hardening phase. And that's another strong plus.

But this tailored approach "is very, very configuration-dependent," notes King, a strong advocate of total shielding. He explains that the vulnerability of a particular system or facility is so dependent on the exact layout of components and even the process used to manufacture seemingly identical parts that any changes in the originally analyzed system could render a specific tailored hardening scheme "for naught." And it has almost become the rule, not the exception, for firms to upgrade electronic systems with minor changes or additions that inexpensively increase the productivity or capability of the existing system.

But there is an even more interesting aspect to the tailored versus Faraday cage debate. "While the tailored guys all agree that the [Faraday cage] approach will work," King says, "not everybody agrees that the tailored approach will." What's more, he says, even advocates of the tailored approach think that when building a new system or facility, it will cost less to shield it in a Faraday cage. So while shielding with a Faraday cage "is not only the soundest way to go," King claims, "it turns out — and I'm doing a lot of work in this area — that it appears also to be the cheapest way to go over the life-cycle" of a system.

Debate over the topic is so intense and vital to issues of cost and hardening effectiveness that the Defense Nuclear Agency will convene a big working symposium on the issue in a few months.

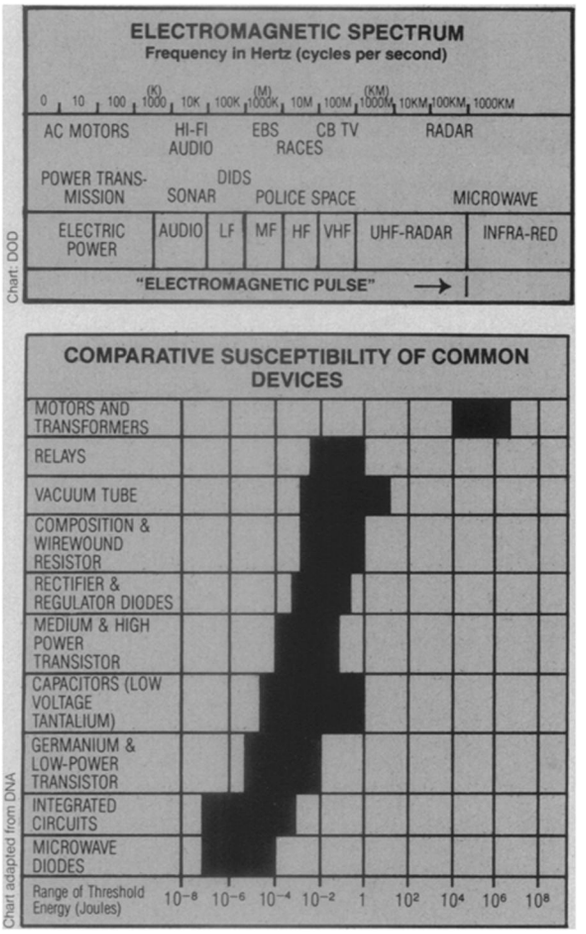
One issue on which there is seemingly no argument is that technology now exists to EMP-harden any vulnerable system.

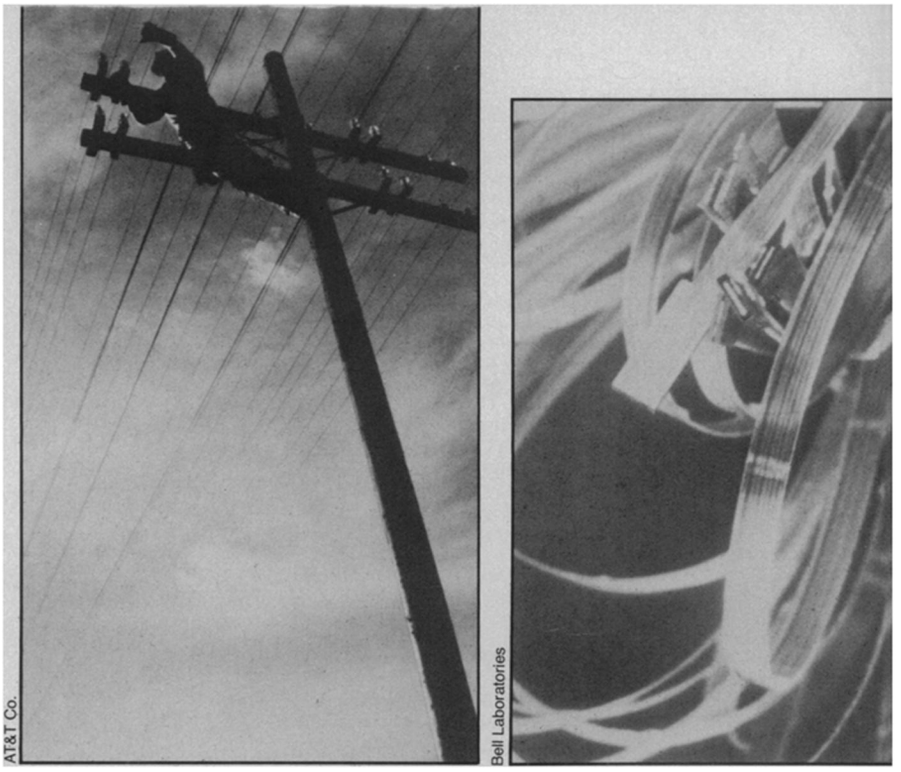
But just because something uses electronic parts doesn't mean that the system is vulnerable. And an impressive survey to narrow down when and why something is vulnerable has been conducted over the past 25 years, largely with Defense Department funding. Many of those studies are still classified, although their results are pouring into the open literature.

For instance, communications equipment using bipolar transistors with self-contained batteries and loop antennas are not susceptible to direct EMP damage. Similar equipment using stick antennas up to 40 inches long is also safe. However, electronic equipment using field-effect transistors could be damaged if the connected antenna is more than 30 inches long. The general implication of these studies, notes the Defense Department in one of its attack-environment manuals, is that mobile communications equipment — including walkie-talkies and the common transistor radio — are relatively survivable in an EMP environment. But radio-transmitting stations will be vulnerable unless expressly hardened for EMP.

"It sort of boiled down to," says Kerr, "if there's no antenna, there's no problem." For example, computers are one of the most vulnerable systems to EMP. But a computer "is not much more vulnerable than a piece of marble," unless and until it's attached to an antenna, the FEMA research director said. And every metal object represents a potential antenna to collect radiated EMP signals and focus them into more massive ones.

That's one reason why FEMA has elected to EMP-harden radio-broadcast stations throughout the nation. Televisions, with their large rooftop antennas and power cords, are prime candidates for EMP damage. But transistor radios aren't, and it has been estimated that 80 percent of the population has access to them. So if, and when, the Emergency Broadcast System is called into use for warning the public about a nuclear attack, an EMP-hardened network of AM and FM radio stations could





Aerial lines of conventional telephone systems (above left) make good antennas for picking up EMP *surges, and the equipment connected to them is vulnerable to interruption by* EMP*'s. Fiber optics (above right), which are coming into use for communications, do not contain the electric and electronic components susceptible to this kind of surge, and so are invulnerable.*

within 10 to 15 minutes broadcast the President or local leaders nationally.

Already FEMA has EMP-hardened 150 to 200 of the 600 radio stations it has targeted to make up its voluntary emergency broadcast network, Sinnott told SCIENCE NEWS. However, since the stations with the biggest broadcast coverage were hardened first, roughly half of the nation is already within earshot of an EMP-hardened station. Completion of the network is expected within three to five years.

Sinnott says that the EBS-network stations will be equipped with backup power-supply systems, usually diesel generators, and fueled to last several weeks. And the anticipated need for that backup electrical power points to what is perceived as potentially one of the least prepared of the nation's industries.

If a high-altitude nuclear blast bathed the nation in EMP, "my gut feeling is...our power systems would probably not be available," says King, whose former employer, the Defense Nuclear Agency, maintains a more than passing interest in that subject. DNA has run "EMP awareness courses" for electric-utility executives and engineers. Still there appears to be a widespread prevailing attitude that lightning arrestors used throughout that industry are more than adequate to tackle the energy delivered by a nuclear EMP.

That's true, concedes King: "Some of the lightning arrestors are more than capable of handling the energy; but they are not fast enough." He explains, as do countless reports and manuals printed by FEMA over the past decade, that a lightning arrestor has to be quick enough to respond to a pulse. The devices — which short out circuits leading into sensitive power-controlled equipment — are designed to handle lightning pulses, which King points out are about three orders of magnitude slower in their rise times than EMP. The result is that an EMP can flash through the circuit, wreaking havoc, long before the circuit can short. While some studies suggest equipment damage could occur, the most likely result of an EMP exposure would be to trip circuit breakers across the nation. Companies with insufficient electric-load-shedding capabilities would be forced to shut generating stations down. "And you're talking 12 to 24 hours to get them back on line," King says. "That's not a damage situation, it's a functional upset. But the effect is the same."

And the net effect is that much if not most of the U. S. power grid would be shut down for hours to days, depending on the frequency with which successive EMP pulses arrived.

"It is necessary to distinguish a rather striking contrast between civil and military approaches" to coping with potential EMP disruptions, explains a 1975 Defense Department study, *Electromagnetic Pulse and Civil Preparedness*. "While the nearly universal military approach has been to harden systems of interest, this is not a feasible civil measure." Military attack and communications systems cannot afford to shut down, even momentarily, during attack periods, whereas "[c]ivil preparedness systems can afford to be out of action for periods running from minutes to days." So while some attempt has been made to harden civil systems, such as the Emergency Broadcast Network, another common strategy has been to analyze likely damage should an EMP occur and then to develop contingency plans to cope. These plans could include storing spare parts that would most likely need to be replaced or simply compiling directions for manually taking over formerly automated activities until repairs can be made.

A number of critics worry, however, that the electric-power industry has been too complacent about the threat of its potential vulnerability to take even these measures. And while the military has aggressively sought to EMP-harden its most important facilities and weapons over the past 15 years, it is quite dependent on several civil systems that appear potentially still quite vulnerable to EMP — notably the nation's electric-power and telecommunications industries. As one EMP analyst points out — in the event of war, these military dependencies on non-EMP-hardened networks could prove an Achilles heel to national defense. □