

The Scariest (Disaster) Book I Have Ever Read, Part III



By [Leo Wrobel](#)

Date: Aug 17, 2011

[Return to the article](#)

The most terrifying weapon facing the U.S. may already be in our enemies hands. Are you prepared for the ultimate disaster? In Part III of his three-part series, author Leo Wrobel explains exactly which systems would be affected by an electromagnetic pulse, how they would be affected, and to what degree

In Parts I and II of this series, we discussed how a single device exploded over the U.S. Midwest could generate an electromagnetic pulse that would destroy the whole U.S. power grid and virtually everything connected to it. Unlike other disasters, an EMP would affect almost the entire nation simultaneously, and dash us almost instantly back into a 19th-century economy. An EMP attack would wipe out computers and the Internet. There would be no electricity, perhaps for years. Emergency services would stop, and hospital operating rooms would close. In the ensuing chaos, most Americans would die from starvation in months

Exactly which systems would be affected, how, and to what degree is the subject of this third and final article

Critical Systems Support Life as We Know It

The physical fabric of the United States is sustained by an organization of systems operating in a complex network of interdependent infrastructures. The inter-relation of these systems enables the millions of actions, transactions, and information flows that enable the conduct of society. Recent disasters including 9/11, Hurricane Katrina, and the Japan earthquake of 2011 have underscored the vulnerability of these systems and infrastructures.

Critical Systems Depend on Solid State Controls (SCADA Systems)

At the same time, use of automated control systems has allowed many companies and agencies to operate effectively with small workforces. And while manual control of many systems is probably possible, the number of people knowledgeable enough to support manual operations becomes more limited everyday.

Stated another way, any repair of physical damage due to EMP or other cause is in most companies constrained by an increasingly small workforce. Today, maintenance crews are sized to perform routine and preventive maintenance of what is generally high-reliability, solid state equipment. When repair or replacement is required that exceeds routine levels, due to a regional disaster such as a hurricane or earthquake, arrangements are usually in place to augment crews from outside the affected area. The simultaneous and far-reaching effects from an EMP change all of this and exponentially magnify the problem. Because responders will most likely be occupied in their own areas first combined with being greatly hampered by the loss of critical services such as communications and electrical power repairs normally requiring weeks of effort may take much longer, perhaps even years.

In April 2008, the report entitled *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* was published. In particular, the commission thought it important to single out growth and resultant dependence in the area of automated monitoring and control systems. These robots of the modern age are otherwise known as *Supervisory Control and Data Acquisition (SCADA) systems*. SCADAs have emerged as critical and growing elements of a quietly unfolding industrial revolution spurred by the computer age. The proliferation of innumerable SCADA systems along with their electronic cousins including digital control systems (DCS) and programmable logic controllers (PLC) affects every aspect of critical infrastructure in the nation. While conferring financial efficiency in addition to flexible operational control, the growing dependence of our infrastructures on control systems like these represents increased vulnerability. EMP affecting such systems introduces vastly expanded, and even exponential, consequences to infrastructure.

SCADAs are electronic control systems that are used for data acquisition and control over large and geographically distributed infrastructure systems. They find extensive use, for example, in electrical transmission and distribution water management, and oil and gas pipelines. Physically, a SCADA system resembles a personal computer (PC). It might contain familiar-looking circuit boards, chips of various sorts, and cable connectors to the external world much the same as any other PC.

Damage to SCADA Systems Has Far-Reaching Consequences

Consider electrical power generation using a conventional steam cycle process. Such a process requires highly complex systems to maximize efficiency while at the same time maintain safety and conform with environmental protection requirements. Therefore, control systems in a steam generating power plant would include parameters such as generator speed, generator lubrication oil pressure, current and voltage output, feed water pressure, boiler steam drum level, air box pressure, and rate of combustion. A malfunction in any of these controls has the potential to cause severe physical damage.

A case in point is the boiler endpoints of combustion and circulation. Normally, the control system would first reach the endpoint of combustion (limit of air and fuel adding energy into the boiler) and thus prevent any thermal damage to the boiler. If the control system is upset, it potentially could reach the endpoint of circulation (maximum rate of steam generation) or endpoint of carryover (maximum rate at which water *not* carried out of the boiler) before the endpoint of combustion. This situation would cause thermal damage to the boiler tubes or physical damage to steam turbine blades.

Everything Breaks Eventually

In 8000 years of human history as we know it, there is nothing mankind has invented that does not fail sometimes. So too it is with our critical infrastructure. Therefore, most critical national infrastructures are fault-tolerant at least to some degree. Design engineers and system managers are cognizant of, and fully expect, failure of subsystems and individual electrical components. Telecommunications and electric networks are designed to avoid single-point failures. Despite everything, the unexpected happens and things break. Single-point failures are anticipated in the design of the systems and engineering solutions of various kinds, including redundancy, rapid repair, replacement and operational rerouting.

Planning for multiple failures, however, particularly within a short time, is much less common. No one has even imagined a scenario with the loss of hundreds or even thousands of nodes across all the critical national infrastructures, all down at the same time. This is precisely the circumstance contemplated by an EMP. This is, in part, why the EMP Commission addressed the following areas in its report:

- Electric power
- Telecommunications
- Banking and finance
- Petroleum and natural gas
- Transportation
- Food
- Water
- Emergency services
- Space
- Government

Critical Systems Are Interdependent

The Commission report astutely pointed out that separation of these infrastructure into different domains tends to obscure the real vulnerabilities—namely, interdependencies between these categories, which support the effectiveness and daily operation of each other system. Consider telecommunications for example. The telecommunications infrastructure requires power that is delivered by the electric power infrastructure. It is anticipated in the telecom industry that power *will* be disrupted due to blackouts, cable cuts, and other causes. That's why the industry has long used backup batteries that supply the 48 volt power used by most telecom components. When power delivery is disrupted, as it often is, telecommunication central offices and their substations will run for a while (up to three days or so for larger installations or central offices, less than a day for Remote Terminal equipment). It

would then need to switch to backup generators powered by diesel or natural gas:

In the case of diesel, the generator's operation would rely on fuel, first from on-site storage and then conveyed to a central distribution point by the energy distribution infrastructure, ultimately ending in the delivery of diesel by the transportation infrastructure to the telecommunications substation paid for by the components of the financial infrastructure. Each and every one of these systems could be compromised by an EMP and thereby affect other systems. We could indeed end up with no phones to fix the power as well as no power to fix the phones!

Modeling and Planning Tools Lag the Threat

No currently available modeling and simulation tools exist that can adequately address the consequences of disruptions occurring simultaneously in critical infrastructures that are as dynamically interdependent as these are. While the federal government is supporting a number of initiatives to develop critical national infrastructure modeling and simulation capability as a national analysis and planning resource, these efforts regrettably are not high priorities.

However, the threat is real. In fact, some analytic work suggests that evolving interdependencies may be introducing new and potentially serious vulnerabilities, even without the precipitating catalyst of an EMP attack. As a result, future vulnerability analysis in this area must include strong interdependency modeling that transcends individual infrastructures. In addition, protective measures should be taken as SCADA systems come in to more and more widespread use.

We Can Refer to Past Practices, To an Extent

Because SCADA systems look and act a lot like personal computers, some 20 years worth of operating and security standards exist on the care, feeding, and maintenance of such systems. Many were published as early as the 1980s by the undersigned. This step could reduce some of the exposure to cyber attacks, for example. In addition, it may be possible to harden SCADA systems against EMP cost effectively through the use of Faraday cage enclosures, such as were discussed in Part II of this series.

As a general rule, SCADA system components are frequently situated in remote environments and/or operate without proximate human intervention. Their critical electronic components are usually confined within some sort of metallic box, which is in fact one component of a Faraday cage. Today's enclosures are redesigned only to provide protection from the elements and basic physical security. They are not designed to protect the contents from EMP.

For one thing, EMP could infiltrate the case from antennas, cables, or other components. Is it possible to build an EMP-proof enclosure? Sadly, the answer is probably no. Is it possible to build an EMP-resistant enclosure? I believe it is. A few dollars spent on materials and new standards for both enclosures and grounding could drastically reduce damage, particularly for equipment in off-grid areas more distant from ground-zero of an EMP attack.

In any case, heightened awareness of the vulnerability of critical national infrastructures caused by the EMP threat to the SCADA control systems is important. We must first develop a sense of the vulnerability of the underlying hardware components themselves from all angles then put the engineers to work. As an example, consider the shielding used in automobile ignition systems. Cars predated radios installed in cars. When radios were first installed they picked up all kinds of interference from the ignition system in the car. Thereafter came new innovations such as improved shielding on ignition wires, resistor spark plugs, and better grounding and shielding on the radio itself. As a result, when is the last time you heard radio static when you stepped on the gas? It did not cost a lot to do either in hindsight. The same kind of effort is called for here.

Worried Enough Yet? Consider Solar Storms

As if EMP was not enough to consider, then how about another threat, let's say from space? Solar storms would primarily affect the power grid, but are not likely to harm things like computers. Solar storms regularly disrupt communications, albeit temporarily, but they would not be likely to cause harm to communications equipment except for satellites. An extremely large solar storm, however, could induce geomagnetic currents that could destroy a substantial number of the very largest transformers on the power grid. That would be a world class problem resulting in a widespread blackout measured in years. Here is why:

According to the experts, unlike nuclear EMP, a major solar storm *will* eventually happen. It has before. The last solar

storm that could have caused this level of damage happened in 1859. Thankfully this was before the power grid was in place, but it played hell with telegraph lines. There is a general consensus that a solar event that is similar to, or larger than, the 1859 solar superstorm will happen in this century. If it happens & we are set up now, without spare: for our largest transformers, a large part of the worldwide power grid (including 7 to 100 percent of the U.S. power grid) will be down for years

A 2008 study by Metatech found that the time that was required to obtain a replacement for any one of the 370 or so largest transformers in the U.S. was 3 years. In a solar superstorm that affects vulnerable areas of the entire world, delivery times could easily be much longer. The United States, which currently has no capability to manufacture those transformers, will be at the end of a very long waiting line. Oh sure, there are some companies in the U.S. that certainly have the capability to manufacture even the largest transformers. Even an expansion of manufacturing capability requires a lot of electrical power that cannot be delivered after an EMP or solar storm. And again, what if there are no phones to fix the power, and no power to fix the phones

Summary

I hope you enjoyed this series and found it food for thought. I still consider this one of the scariest possibilities that faces the contingency planner today, in large part because (like everyone else) I know so little about it. If you have worked on a project for a critical utility, government, or other entity, I would like to hear from you. We may have a spot for you in an upcoming book. Email me at leo@b4ci.com.

See you next time.
