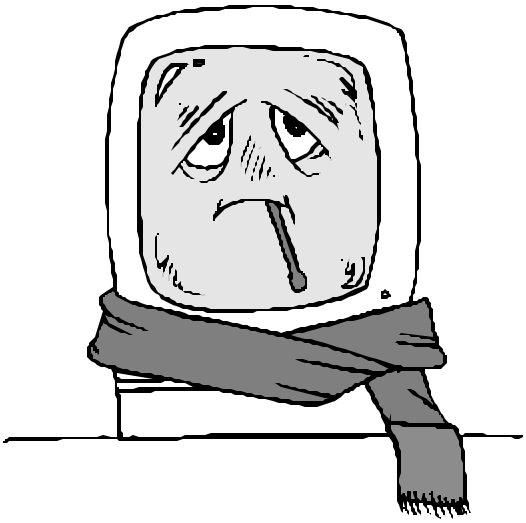
White Paper # 206



Power Viruses
(The Source of Electronic Influenza)

POWERVAR
Solutions for Power Quality

Introduction

Software viruses are common occurrences in the computing world. In fact, almost everyone is familiar with their potential for damage, and the news media routinely reports the details of system disruption related to their appearance.

It's a reasonable term to apply to these rogue programs. They enter a system unseen, often incubate in silence, and eventually come to life with results that range from merely annoying to disastrous.

Electrical disturbances are quite similar. In fact they could reasonably be called "power viruses" since they, too, are unseen and can cause serious and expensive electronic system failure.

Power Virus Origins

Power viruses are contracted the same way as other viruses. They're passed along -- often by your system's electrical neighbors. Plug your system into the wall, turn it on, and look out. You've just been exposed to an epidemic, and there are a lot of very sick electrons looking to cause problems. Some of them may take time to cause noticeable damage. Others are immediately catastrophic (like a lightning strike).

How do power viruses affect an electronic system? What can you do to prevent power viruses in the first place? First it's handy to understand them. Then you can tackle the job of immunizing your system against their harmful effects. There are six main power viruses that can invade a system. The symptoms they cause can vary as can the proper course of treatment.

Voltage Spikes & Impulses

This virus is mostly the result of electrical equipment inside your facility. Electrical loads like elevators, motors, relays, induction furnaces, copy machines, and similar devices can cause sudden large increases in voltage inside the electrical system. Conditions outside your facility can be to blame, too.

Switching activities by the electric utility and lightning strikes can cause transient impulses so intense they literally "blow up" sensitive micro-circuitry.

This virus is deadly to electronic systems -- but not always immediately. Sometimes voltage spikes and impulses are relatively small in amplitude. In these cases, the virus weakens the system components over time leading to deteriorating health and eventual failure. Other times the impulses may be so large that they cause immediate system failure.

Electrical Noise

Like voltage spikes and impulses, electrical noise is generally created inside the facility by the system's electrical neighbors. Almost every electricity consuming device contributes its share of electrical contamination. Things like appliances, photocopiers, laser printers, and electronic lighting ballasts are all noise sources that can cause computers to lock-up, lose data, or behave unreliably.

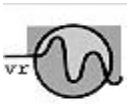
Even computers themselves generate electrical noise. It's truly a paradox that our computers often infect other computers with power viruses.

Common Mode Voltage Problems

Traditionally, this power virus hasn't received much attention. But detection of common mode voltage problems is easier and, as a result, more system problems are being traced to its existence. The condition is characterized by unwanted voltage measured between neutral and ground (the white wire and the green wire or conduit) in the electrical system.

In fact, the common mode voltage virus is probably the most serious power virus infecting electronic systems today. It occurs as a result of high impedance safety grounds, neutral conductors shared with other circuits, and branch circuit lengths that are excessive.

When the electrical noise virus (already mentioned) appears between the neutral and ground conductors it becomes a common mode virus with the ability to cause lost files, system lock-ups or re-boots, communication errors, and "no problem found" service calls.



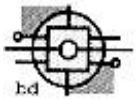
Voltage Regulation

This virus is characterized by abnormal variations in the electrical circuit's nominal operating voltage (120 volts, for example). These variations are generally greater than ± 10% of nominal voltage and may last for several line cycles or more. Traditionally this virus has been referred to as the "sag" or "surge". The virus is typically caused by large loads turning on and off and overloaded branch circuits or distribution transformers. In some cases, voltage regulation viruses can be the responsibility of the power utility. If an electronic system requires tightly regulated voltage (most of today's systems don't) the voltage regulation virus is likely to cause system lock-ups and unreliable operation in addition to damaged or destroyed components.

Blackouts

Blackouts are the most visible and easily identifiable of all the power viruses. And they have the most obvious cause and effect relationship. One moment power is present -- the next moment it's not -- and your system is dead in its tracks as a result.

The effects of unanticipated power loss are obvious. This is especially true if the system is a network or some other "fault intolerant" architecture. Fortunately, in spite of what most UPS manufacturers advertise, blackouts account for comparatively few occurrences of all the power viruses.



Back Door Disturbances

This virus (as its name implies) infects your system via a secondary path. Even though they're not an AC power connection, things like serial ports, telephone lines, network cabling, and I/O connections can all permit power viruses to invisibly enter a system.

This virus causes driver chip failure and communication errors. The back door disturbance virus is often unrecognized. Without treatment, serious damage can occur, and lost productivity can result in substantial financial losses as well.

An Ounce of Prevention

There's an old adage that "An ounce of prevention is worth a pound of cure." Nothing could be closer to the truth when it comes to power viruses. We're familiar with the damage that results from software viruses and we've all experienced the debilitating and sometimes deadly results of real life viruses like influenza. We go to great lengths to avoid both.

In our personal lives, we get vaccinations, eat healthy diets and exercise (most of us), shun contact with infected people, and generally avoid living the type of high risk life style that leads to illness.

Where our electronic systems are concerned, we've learned to practice "safe computing." We back up our data regularly, avoid logging onto questionable bulletin boards and networks, or sharing diskettes of unknown origin. We also run anti-virus programs on a routine basis.

It doesn't require a huge leap of logic to ask "Why don't we practice safe computing where power viruses are concerned?" They have the same potential

effect where our systems are concerned. They enter unseen. They can cause damage ranging from annoying to catastrophic. And like most other viruses, prevention is possible if you understand the basics. There are five simple devices you can use to prevent the equivalent of electronic influenza. All five are required for complete immunity.

The Magic Pill

If there's a magic pill to prevent power viruses, it's understanding that prevention must be practiced as a "system." What that means is that certain prevention techniques must be used together.

Voltage spikes are addressed with a surge diverter and electrical noise with a noise filter. Each of these by themselves, however, is capable only of weakening or slowing down a virus -- not eliminating it.

Isolation transformers eliminate common mode voltage problems. When surge diverters and noise filters are added to the isolation transformer, the resulting "system" kills all three viruses.

Uninterruptible power supplies eliminate blackouts, but in spite of many manufacturer's claims, most aren't capable of preventing other viruses. Once again, the UPS must be used with the other parts of the system to achieve total virus immunity.

The backdoor disturbance can be addressed several ways. Fiber optic connections are one means of electrically closing the back door, but if ordinary copper wiring is used for communication lines, it may be necessary to employ special surge diversion techniques for these connections.

Luckily, the voltage regulation virus is no longer a serious hazard. Once upon a time, this virus was responsible for many system failures. However, today's systems use switch mode power supplies. This technology was designed as a way of reducing both power supply size and cost while simultaneously increasing electrical efficiency. To achieve these goals, switch mode supplies are designed to consume electrical power differently than their predecessors. These operational differences have created a beneficial by-product where voltage regulation is concerned. As a result, most systems enjoy substantial immunity to the voltage regulation virus. Additional preventative measures (voltage regulators, etc.) are unnecessary.

Conclusion

Power viruses are an appropriate description of the power quality problems that can plague electronic systems. Like other viruses, they are invisible -- often announcing their presence only after some initial damage has already been done. Their effects can be a minor annoyance like a lockup or system error or they can be catastrophic like a blown up integrated circuit or power supply failure.

Our dependence on sophisticated technology has created an increased awareness regarding the need to safeguard system integrity. Software viruses have led to the introduction of "anti-virus" programs and system data is routinely backed up to prevent loss. Part of this "safe computing" lifestyle should be the prevention of power viruses, too.

This is possible only when prevention is systematic. Voltage spikes, electrical noise, and common mode voltage is eliminated by a package that contains an isolation transformer, surge diverter, and noise filter. UPS and data line protection can be added to the system as applications demand.