RED/BLACK DESIGN - A DESCRIPTION AND APPROACH

Information Privacy

As Pierce has stated, "Information privacy is an essential element of democratic freedoms and of self-determination in everyday life. Invasion of information privacy, however, is a fact of life".[1] This statement sums up the rationale for why privacy is needed: someone *always* wants to know what someone else is doing or saying. Be it a trade, company, or manufacturing secret, a marketing or financial plan, rosters, or national security information, someone will always be there to eavesdrop, snoop, investigate, or otherwise spy on the unwary. To this end, cryptography has long been used, primarily by governments, to protect and control private, or sensitive information. Its efficiency and superiority over other information security methods is well established and documented. However, the use of encryption to protect information is only one link in the communication chain. Without a diligent corresponding effort to strengthen the other links (and nooks and crannies), using encryption to protect the sensitive or private information is nearly useless.

The RED/BLACK System

Let us assume we have an electronic communications or data processing system which handles information we consider private. The data in its clear, unencrypted form is considered "red", and circuits, components, etc. which help process this data are located in the red portion of our system. All other parts of the system including external control, power, and data lines are considered "black." The actual encryption device will obviously contain a red/black interface between encrypted and unencrypted data. In addition, a red/black interface may exist in any box or system with ports exposed to unauthorized access. The concern is to keep the intelligence-bearing red information where it belongs through isolation or controlled access.

A normal well designed data processing system will not intentionally send data where it doesn't belong. However, components can fail, or circuits can oscillate outside their normal operational bandwidth, and when this occurs the links of our security chain are weakened. In order to keep the links strong, and maintain adequate red/black isolation, two major techniques are normally used.

In order to protect the system from direct component failures, single failure design and analysis is employed. A failure modes and effects analysis would first predict the possible failure modes of all components within the system. Next, an examination of the circuitry would reveal if the possibility existed that one or more of these failures could go undetected during a time when sensitive information is being processed. Finally, the possibility is evaluated that any of the sensitive information might show up accidently on a normal channel at a black interface, and thus become directly available to an unapproved observer.

The second way for private information to cross the red/black interface (and the most difficult to protect against) is by indirect means through conducted or radiated emissions. Since the path is not obvious, many long hours are often required just to find the source of a signal, let alone determine whether or not the signal contains enough information to be useful. This is because useful information is often contained in the phase or amplitude of a particular signal, not just in its presence or absence. A useful presentation on the subject of information theory in secure systems is described by C.E. Shannon.[2]

The purpose of this article is to broadly scope the design areas which must be addressed in depth when a program of information privacy is implemented. An actual design effort would be more structured and specific, since slight deviations could negate the protection afforded to the many interrelated components. In the case of TEMPEST programs, commercial firms should seek specific guidance on the subject through the Industrial TEMPEST Program (ITP) sponsored by NSA before protection related designs are implemented.

Isolation Approach

Isolation between red and black must be considered at all levels from the circuit card to the system. Why is this? Since we are dealing with indirect paths, the mere fact that the circuit cards are separated, wires are individually shielded in a bundle, interface or power lines are passively filtered, or a discrete component is in series in a line, has only limited bearing on whether or not signals can "leak" across the interface. Only through diligent control at each level of the design, system, rack, and box, can a "warm feeling" be gained that the sensitive information will be protected. It is a serious mistake to assume protection can be achieved in an "after the fact" effort.

System to Rack to Box

In general, red/black isolation at the system level is usually accomplished by adequate isolation of the power system, and implementing a single point ground approach. Red and black cable runs are physically separated with the red bundle shielded. Often fiber optics are employed to provide total isolation and decoupling. Red equipment areas (REA's) or control zones are used as a means of physically protecting the system from unauthorized access. In this case black lines which physically egress the zone require filtering for both common mode and differential mode signals. When telemetry equipment is employed within a control zone, antenna isolation often becomes a major concern requiring a significant protection effort. Figure 1 shows a typical controlled data processing system.

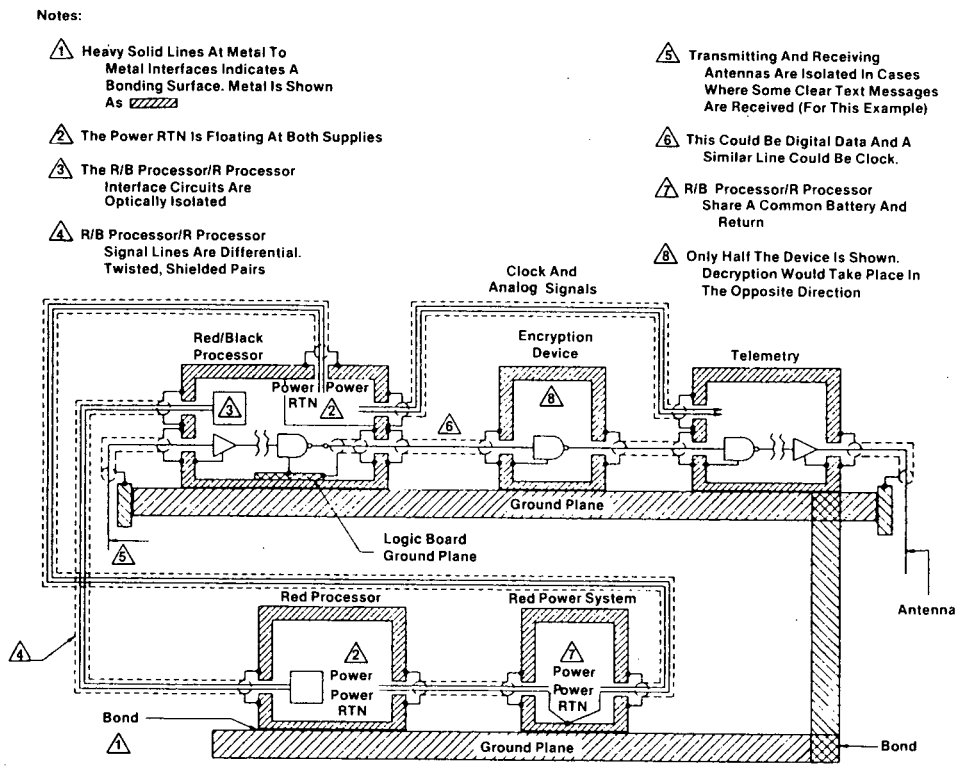

Figure 1. Typical RED/BLACK System Layout.

Rack level red/black isolation is easiest to implement when all equipment in the rack is processing red data. Black and red equipment should not be intermingled within one rack, and each rack type should be physically separated. The multitude of grounds for each equipment box are difficult to control, with usually a common power ground point required near where the cables egress. Power cables and control or signal cables should be routed separately within the rack. Guidance by highly qualified people is necessary in most situations if extreme isolation such as required for TEMPEST is to be achieved.

Cable and connector coupling can be prevented by maintaining the integrity of red grounds, using TSP's, bonding 360° between braid and backshell, using double shielded outer braids, avoiding pigtails, using fiber optics, and compartmentalizing connectors and backshells. Typical connector pin isolation is shown in Figure 2.

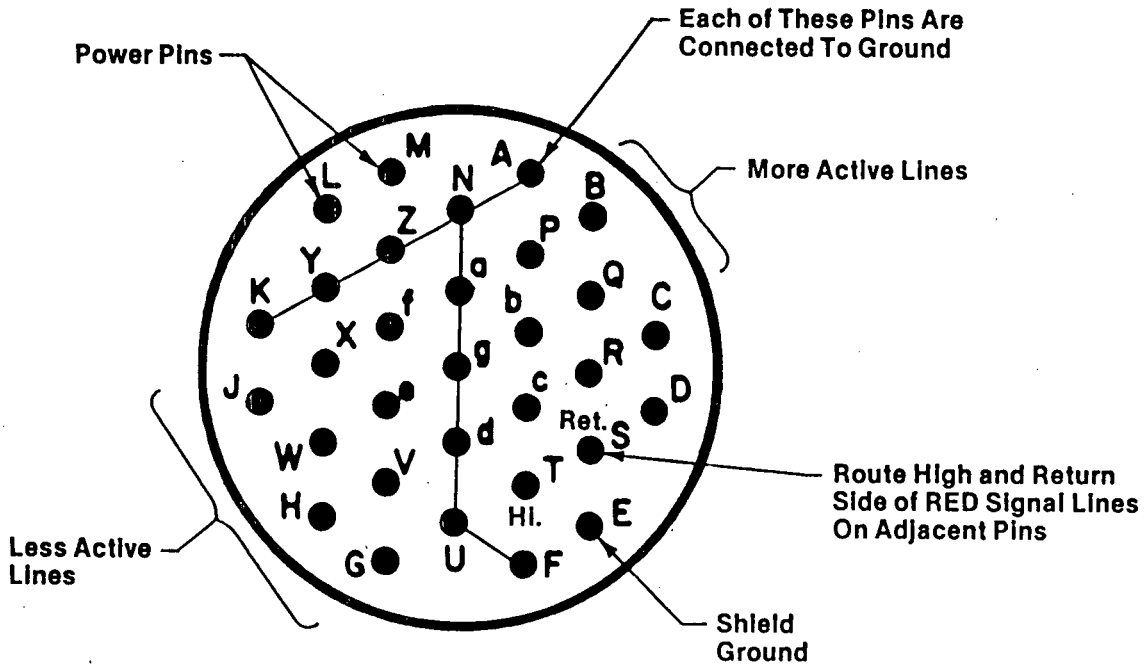

Figure 2. Connector Pin Distribution.

The most effective application of isolation transformers is with racks of equipment. A rack acts as an outer shield for internal instruments, while serving as the zero-signal reference for system output signals. Isolation transformers are used to control shield currents, and to break up the mutual capacitances between rack instrumentation and an unknown power ground. These capacitances are the primary path by which significant powerline and transient related noise couples to the rack, or red signals couple out of the rack. An isolation transformer will eliminate common-mode coupling and reduce most transverse mode coupling.

A common approach is to treat the rack of red processing equipment as a node, then use shielded doors and filter the lines into or out of the node. This approach is primarily used when

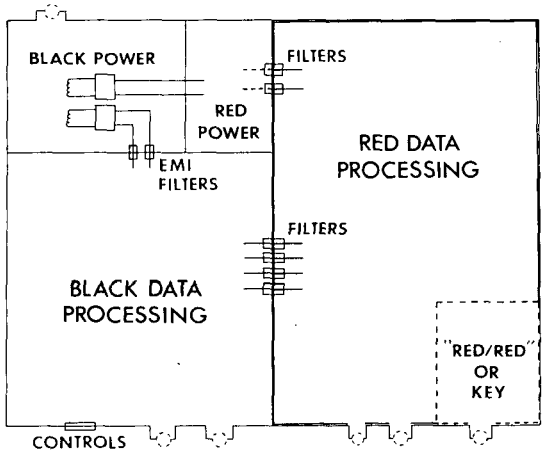

Figure 3. Typical RED/BLACK Partitioning.

dealing with commercial equipment not designed to meet TEMPEST applications. By *not* controlling grounds within the node, ground loops often are created which can cause the rack walls or door to re-radiate the signal being isolated.

Red/black isolation most often occurs at the box level. The chassis provides the overall outer shielding with dipped braised usually recommended. Covers are grooved and gasketed, viewports or holes are covered by mesh and employ waveguide techniques, manual controls and indicators are isolated and in front of the box. Internal partitioning is required with the most common design being power transformers, power regulators, black circuits, and red circuits, located least to most protection from front to back. This arrangement is shown in Figure 3.

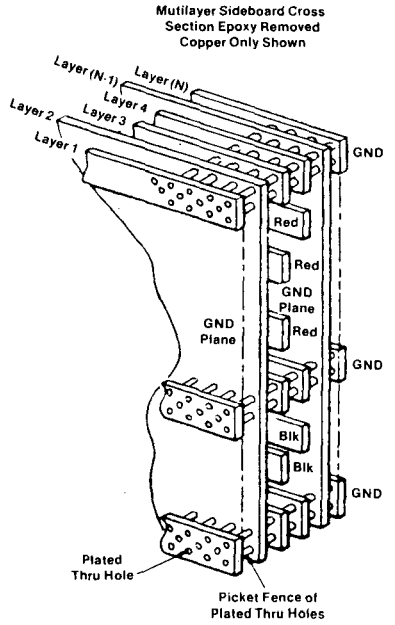

Figure 4. Picket Fence RED/BLACK Barrier.

Motherboards also require isolation and partitioning. Wire-wrapped boards should be avoided. If used, braid shielded wires are required on highly active lines. The best approach is to use multilayer boards with outer ground layers and an inner power plane. "Picket fence" isolation should be used. The technique is shown in Figure 4. Active and passive filtering between compartments is required. Figure 5 shows how filters are used to route lines across the picket fence. Circuit cards should use the same multilayer ground and power plane design. Active or power consuming devices should be located near the card connector and away from other circuitry where possible. One should never place red and black circuitry on the same card. Figure 6 is a typical ½ ATR sideboard layout with barriers.

Isolation amplifiers are often used to isolate signal input from signal output and/or power input. Isolators eliminate ground loops, and have excellent common mode rejection. Capacitance coupling within the devices usually limit their application to the low kHz range.

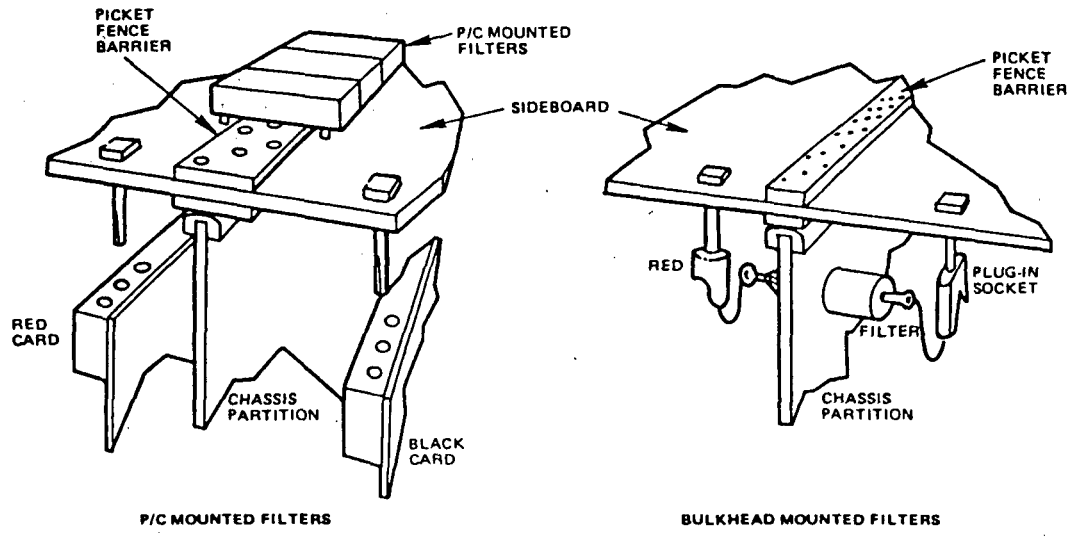

Figure 5. Filtered Compartment Interconnection.

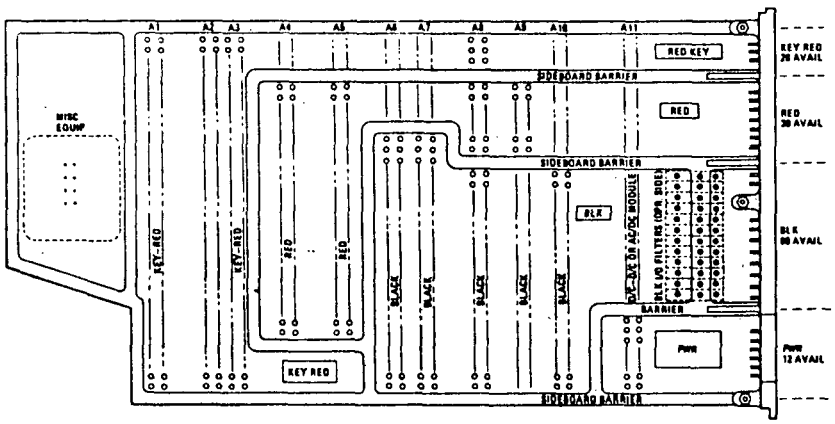

Figure 6. Typical Sideboard Layout with Barriers.

Power Supplies Are Trouble

Power supplies not only are a source of noise, but usually represent the biggest problem when isolating red and black within a box. Almost all red boxes have their primary power-line in a black area. Therefore, the red/black interface often is located within the power supply. Several techniques are used to reduce power supply noise and isolate red power from black power. The more exotic techniques are required when a high level of isolation is necessary. Briefly, some of the more common techniques are presented here.

Internal battery power is preferred, but dc power must be dc to dc converted after rectification within the box. Also, re-regulate the power when going from black power to red power. Transformer coupling provides dc isolation between input and out power, but to prevent radiated emissions, shield the transformer. Separate secondary signal and power wire distribution to sensitive circuitry, especially in cable bundles. Even though less efficient, shunt regulation is preferred over series regulation since series regulation only isolates in one direction. Reduce switching regulator efficiency to prevent PWM from indicating data transfers. Multipoint grounding for power supply circuits is often necessary. The switching frequency should be synchronized to the reference oscillator, a higher frequency preferred.

Insure harmonics and their cross modulation products do not fall within RF circuit bandwidths. To reduce switching transistor noise, the following design techniques are often employed. Reduce collector to heat sink capacitance. Slow down the drive transistor or switching transistor turn on. This prevents high frequency oscillation and reduces transformer saturation by adding delay capacitance to the transistor base. Optically isolate the feedback loop. Remember, if very little noise is sent into the processing circuitry, few carriers will be available to be modulated, shock circuits into oscillation, or otherwise create isolation problems.

Interfaces

Interfaces are often the only area where significant red/black design protection is employed. This is sometimes due to an improper interpretation of the problem by program managers or circuit designers who feel their design is above reproach, and only the interface is suspect. Since there aren't a lot of things that can be done to an interface, some companies even feel that any design engineer can solve the red/black isolation problem using filters, shielding, and well designed interfaces. While systems can and sometimes do meet their contractual requirements using this approach, the costs and time involved to fix problems after the fact usually far exceed the costs of doing a complete design the first time through. If TEMPEST requirements are imposed, the contracting organization is responsible for providing specific guidelines at the time of award, or as soon as possible thereafter.

Twisted pairs will generate minimum noise. The true twisted pair should not be confused with a single ended driver and a ground return wire. Also, attention should be paid to the offset voltage if maximum field reduction is to be achieved. Optoisolators will prevent common mode coupling. CMOS generates the least internal noise, but these devices are insufficiently isolated for use in digital filters. The interface filter should contain saturating logic such as TTL or LTTL. Parallel data transfer is the preferred technique. An op-amp using band width limiting and automatic gain control is often used in series with the data line prior to the interface. A typical filter crossing the red/black interface, and a typical external interface design are pictured in Figures 7 and 8.

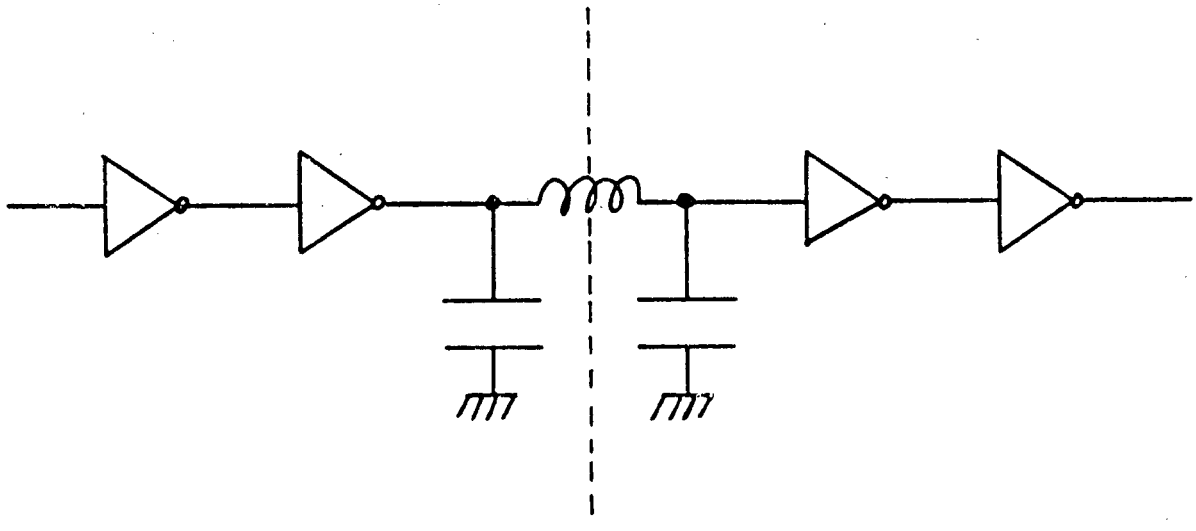

Figure 7. Internal RED/BLACK Digital Interface Projection.

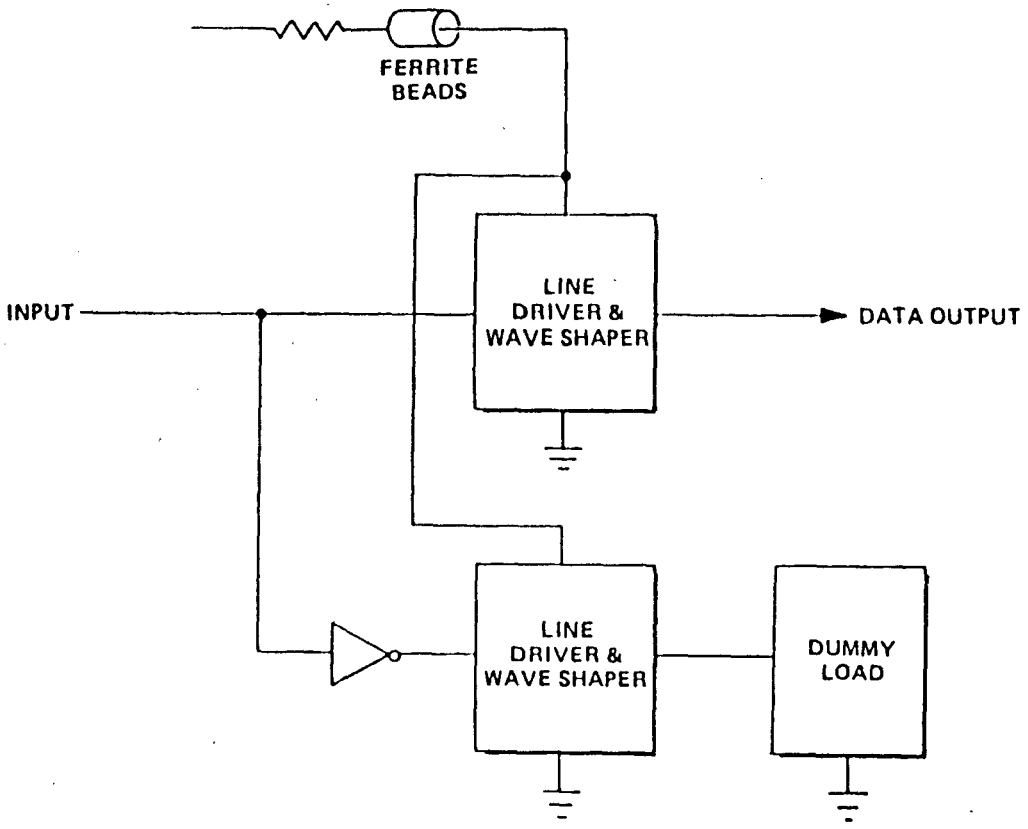

Figure 8. RED/BLACK Conceptual Interface.

Conclusion

The information contained herein is only intended to address the scope of the red/black isolation program. The complexities of the subject (especially with TEMPEST) are numerous, and cannot be addressed with the brief overview presented here. True protection begins at the first step of the system definition phase, and requires a diligent and concentrated in depth effort by experienced people throughout the design, production, and qualification phases of the program. In keeping with the position that the best defense is a good offense, the best and often required approach is to start at the beginning and do security design right the first time. It is suggested the reader contact the National Security Agency if more specific TEMPEST related information is required.

References

1. Pierce, Clayton C., *Secret and Secure Privacy, Cryptography, and Secure Communications,* Ventura, California, 1977.
2. Shannon, C. E., *Communication Theory and Secrecy Systems,* Bell System Technical Journal, pp. 656-715.

This article is based on material from the teaching seminar, TEMPEST: Description and Application, *by Bruce C. Gabrielson, Lead Engineer and Group Leader of EMI/TEMPEST Engineering, Aerojet ElectroSystems, Azusa, CA. Mr. Gabrielson adapted his lecture notes for this* ITEM '84 *article.*