Issues in Firing System Safety

27 September 2011

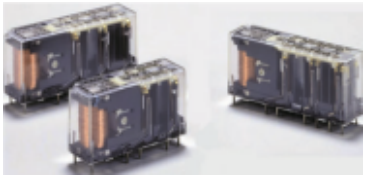
The purpose of this memorandum is to identify faults in contemporary firing system construction which can lead to system failure, in particular failures which can result in damage to personnel or property. Failure of the system to fire, while impacting the quality of the show, has a low probability to result in damages. This memorandum, therefore, will deal primarily with issues that result in unintended firing of a pyrotechnic effect, and will deal with failure to fire as a secondary issue.

In our Fault Tree Analysis (see Appendix A), the primary fault is therefore identified as unintentional release of more than 100mA of current through any combination of input/output terminals connected to electric matches. While most electric matches used in pyrotechnics have an All-Fire Current rating of 500mA (i.e. the match is specified to fire at or above 500mA) and a specified No-Fire Current rating of 200mA (i.e. the match is specified not to file at or below 200mA) many companies do not have an exemplary record of quality control, especially new matching coming out of Asia. For this reason, we have narrowed our analytical requirement to 100mA.

Table of Contents

Design Considerations Impacting Primary Failure Conditions

Relays



Relays, being mechanical devices, are capable of switching high current loads, and often require high energy actuating currents, which makes them practically immune to control transients. Alternatively, they are susceptible to mechanical transients, which are common in pyrotechnic environments in particular. Anecdotal examples of recent relay driven firing systems out of China which can fire from mechanical stress as simple as the thump of a large mortar firing or dropping the module on a table exist as examples of this effect. Even seismic events (common in California, for example) may be sufficient to cause inadvertent firing, if struck at just the right time. Even so-called "safe" relays have their limitations. For example, Omron Safe Relays [1] have a Malfunction Limit of 100m/S^2. This limit can conceivably be breached by the blowout of a nearby mortar or low break shell. In addition, the relays are only specified for operation at relative humidity limits of 85%. Usage of relays in venues or environments that impose stresses outside their specified limits can negate the implied liability coverage of the units.

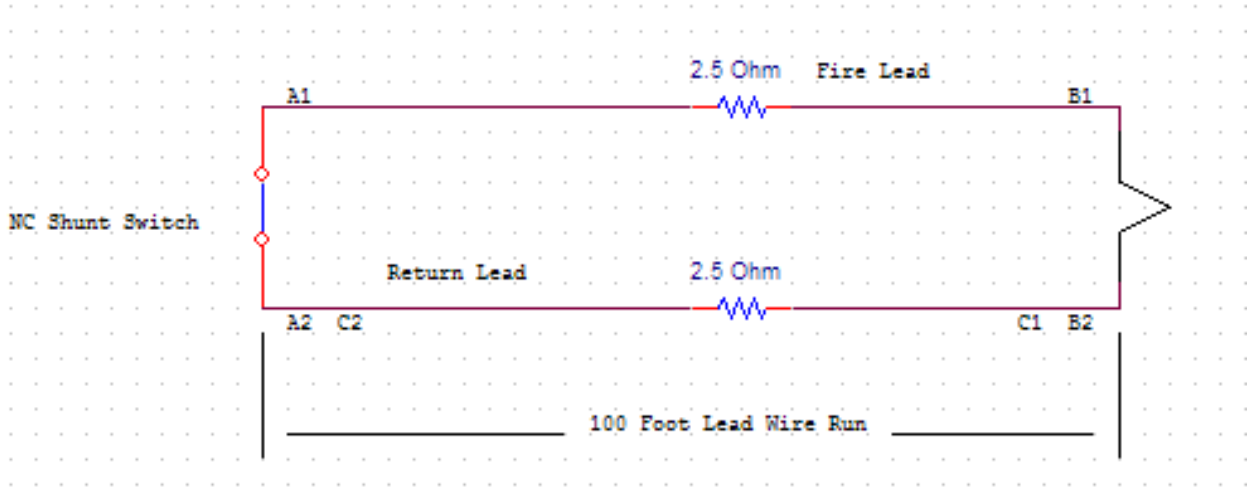
It will be shown below that the load switching and high energy actuation requirements which make relays a desirable option can also be achieved in solid state electronics without the attendant danger of mechanical mis-actuation, and as a result relays should never be used in pyrotechnic environments.

Cross Coupling between Outputs

Cross coupling between outputs is a well documented (see Appendix B and [2]) and understood problem. The omission in providing a solution is usually one of purely economical considerations. In addition to the problem of cross-coupling the excitation signal of one e-match with another, other less common cross-coupling potentials also exist. For example, pure water is a good insulator, but when water is doped with salts, minerals, or other contaminants, it becomes a conductor. This is why it's not a good idea to use your hair dryer in the bathtub. The atmosphere is full of these kinds of contaminants, rendering even rainwater problematic. If the connectors or wires carrying the firing current to the e-match are exposed to water, cross-coupling can result. In many firing systems, no consideration is made to the attack and delay slope of the firing signal. It is simply switched, either mechanically or through solid state (MOSFET switches for example) and the result is a square wave. When a square wave moves down a long transmission line such as the wiring used between the firing controller and the shell, it radiates a wide range of frequencies which can cross-couple into other parallel lines running adjacent to it. Often spare wire is also coiled up, with multiple bundles of wires in the same coil, resulting in quasi-transformers which can accentuate the effect.

Additional faults can be induced from long wire runs. If we assume a scab wire run may be 20 to 200 feet, and the commonly used wire is 2 conductor 24 gauge, the resistance of 24 guage is 25 ohms /1000 feet. So, 100 feet = 2.5 ohms

Obviously, it will require 2 faults to cause current to flow in an isolated circuit. One must provide a voltage and current source and the other provides a current sink, usually ground. Assume a worst case condition. The fire lead of an adjacent circuit is directly shorted to the isolated and shunted firing circuit. And a good, i.e. low impedance, fault to ground.



Case A

On the schematic A1 Voltage/current source; A2 ground fault contact

Both are located near the shunt. Shunt provides a low impedance path to ground, so, very low voltage across leads to match and the match does not ignite.

Case B

On the schematic B1 Voltage/current source; B2 ground fault contact

Both are located near the Match. The match provides a 1.5 ohm path to ground, in parallel with 5 ohms wiring resistance, so, almost all current goes through the match and the match probably ignites.

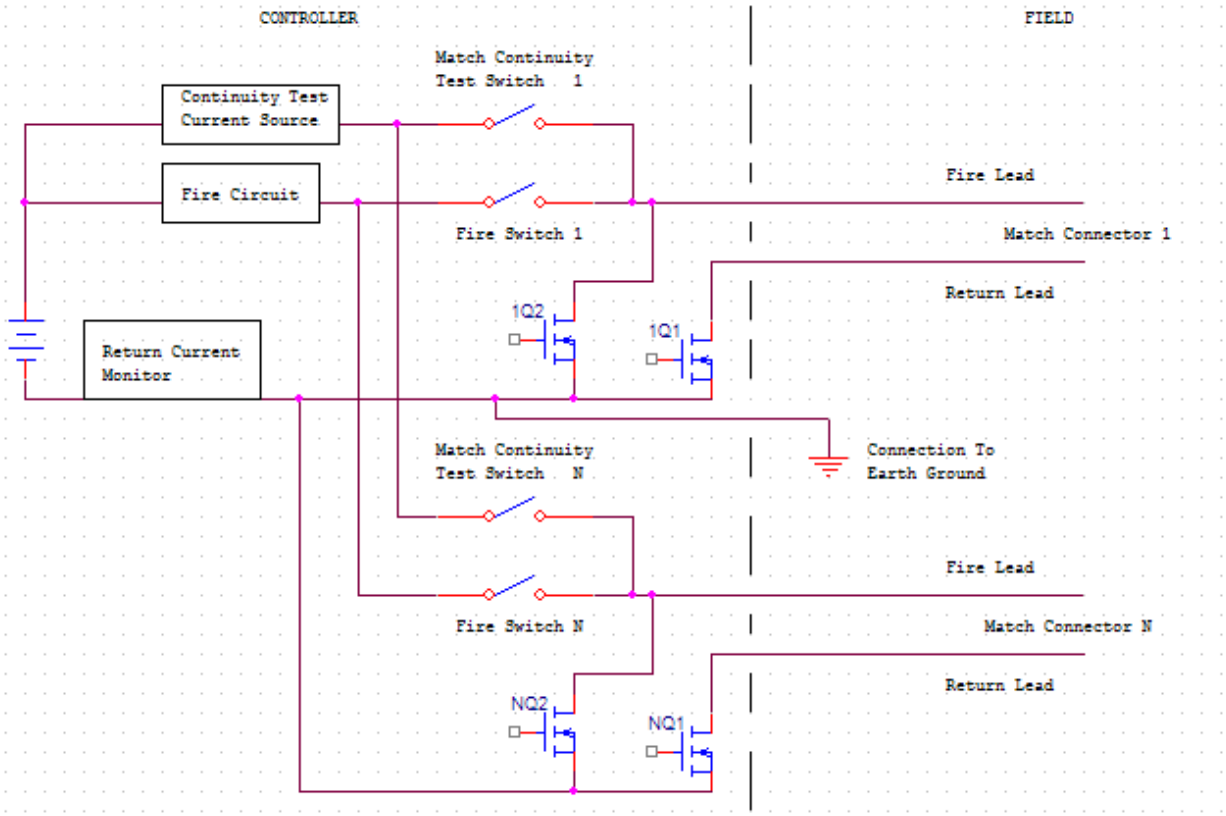
Case C

On the schematic C1 Voltage/current source; C2 ground fault contact

Both are located on the return lead. The Voltage/Current source is located near the match and the ground fault is located near the shunt. This provides 2 parallel current paths to ground. One path is a series through the match, the fire lead and the shunt to ground with a series total resistance of 4 ohms. The other path is through the 2.5 ohm return lead to ground. This means that approximately 60% of the available current will flow through the return lead. The balance of 40% will flow through the match and it will probably ignite.

IMPORTANT NOTE: In this case, the pyro misfired because of the shunt. The shunt provided the current path to fire the squib.

In adding a shunt to the match, as shown above, secondary effects can be introduced. In order to avoid the use of relays, it is recommended instead that both the hot and return lines of the match be shorted to ground through an FET with logic level gate (to prevent glitches in the gate circuit).



This configuration provides protection against external excitation to the match during setup, but if the shunts are left in place during firing, they provide another ground path for a cross connection. It is therefore recommended that at the point where continuity testing determines that a match is connected, or at least before firing commences, the shunt be removed.

This configuration provides an additional benefit. Note the addition of “Return Current Monitor” next to the battery in the diagram above. The first test is preformed immediately prior to installing the pyro charges. Its function is to detect any connection to the fireside lead of all channels. Without the match being installed, there should be no connection to earth or any other circuit. This test should be done sequentially on each fire channel.

To perform this test :

On the channel being tested

1Q1 On to connect return lead to ground

1Q2 Off

On all other channels

NQ1 On to connect return lead to ground

NQ2 On to connect fire lead to ground

Apply Continuity test

If no current detected, Fire lead OK

If current detected, Unintended fault, so, take corrective action

When all channels are clear, install pyro

Perform match continuity test (1Q2 Off, 1Q1 On) to verify all products are installed properly

The second test should be performed immediately after continuity verification and also just prior to the show. The installed match now provides intended continuity between the fire lead and the return lead. So, we can now test for faults to the return lead. This tests function is to detect any unintended connection to the return lead of each channel. And also, it rechecks unintended continuity to the fire lead. This test should be done sequentially on each fire channel.

To perform this test :

On the channel being tested

1Q1 Off to isolate return lead from ground

1Q2 Off

On all other channels

NQ1 On to connect return lead to ground

NQ2 On to connect fire lead to ground

Apply Continuity test

If no current detected, Return and Fire lead OK

If current detected, Unintended fault, take corrective action

Switching Power vs. Switching Ground

Another engineering decision that directly affects safety is whether to supply common power and switch the ground connection, or use common ground and switch the power connection. In a perfectly closed system, switching ground would not be particularly problematic. However, in the real world systems are rarely perfectly closed. Coupling from wiring which is seldom insulated at the splices has already been discussed. Another potential grounding issue arises when power to the system is provided not from an isolated battery an external mains or generator supply which can provide an earth ground. These sources of cross-coupling can provide current paths from the common power rail to any potential coupling fault.

Ground Isolation

Even when switching power instead of ground, care should be taken to make the current paths as closed as possible. The cases of the main control and firing modules are often metallic because of potential incendiary issues, and one way or another the case is often coupled to the circuit ground of the firing electronics. Given the myriad of conditions and structures that may impinge upon these modules, the cases should be electrically isolated from the firing circuitry. In some cases, however, Earth grounding is desirable, so a grounding lead should be provided.

Single Point Failures

Single Point Failures (SPF) are defined as any point in the electronic circuitry ***or the attendant embedded software*** that can, if that point fails, result in our primary failure condition. We will deal with the software aspect of SPFs below. In contemporary firing systems the most common SPF results from energizing the firing circuits. Some systems must energize the firing system when they are plugged in, because the electronics and firing switches share the same voltage source, or they are energized at continuity testing.

Output Driver Stuck On

Once the firing circuits are energized, a common failure is that the output driver is stuck ON, or in the conducting state. The firing circuit in some systems can be a simple P- or N-Channel MOSFET transistor (depending on whether the system switches power or ground. The least expensive system is to use an N-Channel MOSFET to switch the common power to a specific ground line). If this transistor fails, it can fail either ON or OFF. While OFF is the most likely failure, the probability of ON failure is significant. If the device has failed in the ON-conducting state, unintended current release will occur as soon as the firing system is energized.

Output Driver Control Glitch

Control Glitches are another single point failure which can occur whenever the firing circuits are energized. MOSFET switches were developed for applications where very low currents and voltages are desirable to control either saturation mode switching or amplification applications. Because of this, they can be switched at voltages as low as 0.8V and 250uA (.00025 Amperes) of current. Another measure of the susceptibility of the switch to momentary control transients is to consider the amount of overall energy required to trip the switch into conductivity. For the above MOSFET, the threshold energy is

given by the manufacturer as 0.72nC (nano-Coulombs) of energy. In converting this to Amperes/Second, a transient activation signal of only 2.88uS (0.000002 seconds) is sufficient to trigger conductivity. It should also be noted that these simple switches also produce square wave outputs, mentioned as being problematic above.

In contrast, more complex switching circuits often known as "intelligent switches" are available, and while more expensive, these are used extensively in automotive and other mission critical safety applications. Intelligent switches are intended for applications where control of the switch and its output are the primary considerations. The input requires a voltage of 3.25V for a minimum of 30uS to activate, which works out to activation energy of 330,000,000nC or 458,000,000 times the activation energy of a MOSFET. This makes activation by transient vanishingly improbable while simultaneously providing control of the attack and decay rates of the signal to prevent square wave transients and protection against overheat conditions and impulses from external static electricity.

Continuity Test

In the implementation of a pyrotechnic event, the fireworks shell or special effect element is most often attached to an e-match, and then the e-match is wired to the firing module and from there to the master controller. Many variations on this theme exist, but the primary design consideration is the question as to how to detect wiring failures. These wiring failures most often result in the shell not firing, but they can also cause cross-coupling so that the wrong shell fires and this can lead to our primary fault condition, the release of an effect that can cause damage to persons or property. The continuity test is designed to send a small current through the electric match to determine if the wiring has been connected, or if the circuit is still open. This simple test catches most problems for low cost, but does not, and realistically cannot, determine if the shell attached to the terminal is the right one.

Most systems do not consider an SPF in the continuity test to be a critical failure as per our definition, because firing regulations (see Appendix 2) require all personnel to be cleared from the area before continuity testing can be performed. In practice, this requirement is nearly impossible to implement and is regularly ignored in the industry. But even knowing this some systems feel this regulation absolves them of responsibility for safety in this matter. If one is to construct a firing system to be used in the real world, all realistic safety factors must be taken into consideration.

The most common SPF in existing designs is the design of the continuity test circuitry. This necessary component of a pyrotechnic firing system provides Single Point Failures through two mechanisms: First, in some systems the firing system power must be excited in order to perform the continuity test. This results in SPF conditions in the firing components as outlined above. Secondly, the key term in describing the functionality of the continuity test is a ***small*** amount of current being sent through the electric match to determine circuit connectivity. If the amount of current going through the match becomes large enough, or is applied long enough, it will fire. Therefore the design of the circuitry to perform the continuity test must also consider any SPF within that path. In the blasting industry, this is termed "Intrinsically Safe" [2], and is defined as a design where at least two components must fail before the functionality of the circuit is compromised. Therefore no Single Point Failures can exist.

Whenever possible, the power source and circuitry for the continuity test should be isolated from the firing circuitry as much as possible to prevent cross-coupling between the two functions or the creation of SPFs.

Another safety feature usually missed in conventional firing systems is limiting total current through the continuity tests to the safest levels possible. In some systems, the current running through the match is used to illuminate an LED, as the indication of a good circuit. This presents the designer with conflicting goals: Continuity testing is often performed in the daylight hours of the show, so the LED must have the highest power possible to make it visible. For safety, however, the continuity current should be as low as possible. This is complicated by the number of channels that are being checked. If 32 channels are to be allocated 20mA each for continuity testing, the total system current is 640mA, well above the 500mA All-Fire threshold of the e-match. If an SPF exists in the continuity test circuit that could release all of that current through a single match, our primary design fault could occur.

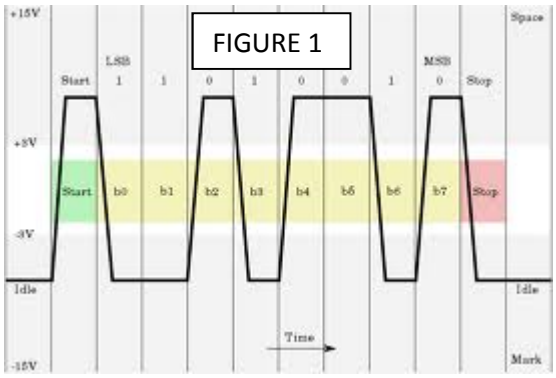


FIGURE 1

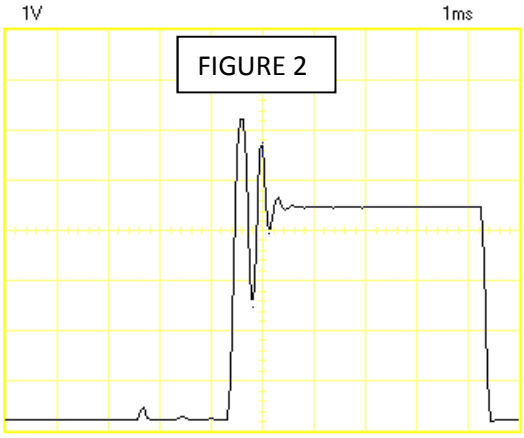


FIGURE 2

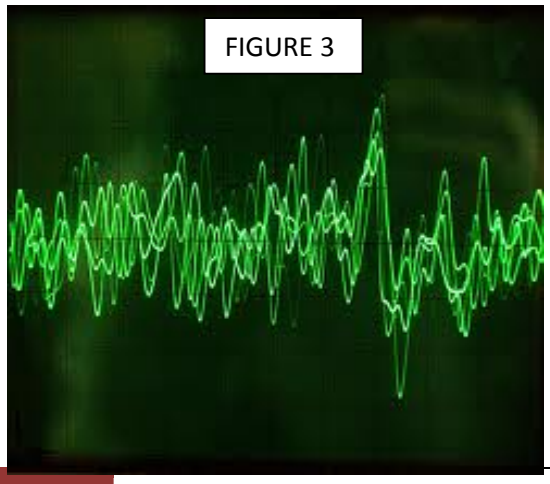


FIGURE 3

Communications

In addition to failures in the hardware circuitry itself, communications failures can be a contributing factor to our primary fault. If the firing module mistakenly interprets a message as a firing order, the results can be catastrophic. This has been demonstrated in simplistic systems which use circuitry intended for garage door openers or baby monitors which are easily fooled by spurious noise and interference. Other more complex communications problems are:

Ringing

In some systems, a simple 16-bit digital command sequence is sent down a long transmission line. The sequence contains the address of the module which is to respond to the command, and the command itself. In some cases, a more complex digital signal is superimposed on the power line of the system itself, so that both are connected at the same time. Due to transmission line effects, the square waves often used to transmit binary information become more rounded and the slew rate (the attack and decay of the wave) is slowed. At junctions where the transmission line is interrupted by a splice or a connector (such as the

connector at the firing module) the signal is also reflected, causing reflections of the signal to travel back down the transmission line and interact with the original signal. In Figure 1, an example of a simple 8 bit digital transmission signal is shown. Any signal conforming to this basic configuration will be interpreted as a valid message. When the module is first connected to the transmission line, and that connection also applies power to the system, ringing or other interference spikes can occur. Figures 2 and 3 show some waveforms of common ringing and noise phenomena. While an event of low probability, it has been repeatedly demonstrated that firing modules do sometimes fire one or more circuits immediately upon connection to the power system.

Random Interference

In terms of probability, the complexity and robustness of the communications system used between the master controller and the modules must be considered. The simpler the communication strategy, the higher the probability of error will be. Garage door openers use 8 to 16 and sometimes 24 bit codes. Wireless systems that use tones are often even more probable to random interference as their equivalent bit complexity may be as simple as 4 to 7 bits. A transmission that does not contain within it a way to check the validity of that message must be considered a Single Point Failure. For example, most integrated circuits intended for digital message transmission include at least a parity bit. In this technique, when an 8 bit message is transmitted, for example, a 9^{th} bit is also sent that always makes the total number of bits an even or odd number (depending on the scheme). This provides a check so that if a totally erroneous message is received, or even just one bit of a valid message is corrupted, the 9^{th} bit can be used to detect that the message is not valid. In this simple parity system, two error bits would not be detected. Error detection and correction has been extensively studied in the last 50 years, and a critical system such as a firing system must use such technology to validate the transmitted commands.

In a 16 bit transmission system, the odds of failure due to signal corruption are probably only in one in the thousands, or tens of thousands, and only marginally better with a single parity bit. By contrast, in modern packetized communications protocols, a message may 256 Bytes (2048 bits) or longer and contains an 8 or 16 bit Cyclic Redundancy Check (CRC) which is used to detect multiple bit failures. The odds of a random failure (undetected corruption) of this type of signal can be as high as 10 to the 77^{th} power, which is roughly equivalent to the number of hydrogen atoms in the universe.

Another important transmission technique which can be employed is encryption. If two wireless modules of the same make are transmitting in the same area, some methodology must be employed to ensure that the transmission of one system, which will be properly defined and formatted, are not mistakenly processed by another.

Condition Detection

Unless a fault condition can be detected, it must be assumed for fault analysis that it exists. Once the firing system is energized and designed interlocks and backups are removed in order to finally – intentionally—fire the circuit, some single point failures can still exist. Some minimum recommended detection points are:

1) Good Power Condition – battery status or power supply status is good. If the power supply is unstable, the system is unstable. In addition to being able to measure the system voltage level, it is recommended that under voltage conditions initiate system resets or full power downs, and glitch or transient voltage conditions, which occur most often when external power is provided to the firing module and that power supply is shared over multiple modules, be monitored so that if the transients are frequent or severe they can initiate system reset or power down, or at least provide warning to the operator.
2) Firing system voltage. In addition to simply knowing if the firing system is energized or not, detecting intermediate levels can indicate other problems such as stuck-on output switches.
3) Output voltage (one per output channel). This detection point often exists because it is required for the continuity test. In many systems, however, it is a simplistic Pass/Fail test. Some power level is applied to the output channel, and if the circuit is open that power level is detected in the test. If a low-resistance e-match is attached to the output circuit, the measured voltage will be lower. With slightly more intelligence designed into the circuit, we can measure actual resistance of the wires attached, and detect more errors, such as too much resistance on the wire, or the improper number of e-matches on the output, which could indicate improper or cross-wired conditions, or some shells that should be wired and are not.
4) Software/Hardware Interlock Mechanisms. As will be shown below, it is often desirable to use physical hardware to add interlock mechanisms to software, to prevent software SPFs.
5) Partial failure of the Intrinsically Safe continuity test mechanism. Any system with redundancy can degrade over time if some components of the circuit fail. Because of the built-in redundancy, the circuit continues to perform, but eventually the configuration of a Single Point Failure will be reached. Some mechanism of detecting a partial failure of the continuity test protection circuit should be provided.

Timing Fault

Another potential failure, unintended release, could be the result of timing problems, such that the right shell is fired at the right place, but at the wrong time. In most fireworks display venues, this would be a minor inconvenience as all personnel should be cleared and observing safety precautions, but in close proximity work where performers may be dangerously close to the effects at predetermined times, it would meet our fault definition. Practically, it is also sometimes that case that safety personnel are sent into the field to solve problems or deal with dangerous conditions that may arise, and having shells go off at unexpected times could also be problematic.

Timing faults are most often caused by improper timing information being transmitted to the system controller, the firing modules, or both. For example, in some systems the time code is provided by some external device such as a CD player or SMPTE timing generator. How the system reacts to errors in this transmission can trigger our primary fault definition. For example: If, by operator error, the time code player is started in the middle of the show instead of the beginning. If the system responds by trying to "catch up" to the time it is being sent, all of the shells in the first half of the show would be fired. In some anecdotal cases, this has resulted in most of the show being fired unexpectedly. Systems should

always use their own internal clocks, and provide safe and deterministic methods of reacting to changes or unexpected values in the incoming timing stream.

It is also often the case that the timing input code has bit errors in transmission. This has been particularly problematic in SMPTE systems, but can occur in any system. Again, if the system does not react properly to random and spurious faults, it can result in an unintended release.

PCB Circuit trace fault

In almost all cases, a fault in a PCB circuit trace results in an open circuit, not a short. It takes very little mechanical motion or degradation to open a circuit trace, but because of minimum separation rules there must be contributing factors such as part misalignment, tin whiskers, corrosion coating, etc. before a spontaneous short between traces can occur. We will, therefore, treat the probability of a spontaneous circuit trace short as vanishingly small and deal with the contributing factors below.

Open circuits, however, must also be analyzed as SPFs that could contribute to our failure scenario. For example, during power sequencing of the device, the logic state of many control lines are unknown for some amount of time while the power level stabilizes, the processor comes out of reset, and the control lines are initialized to the proper state. In order to guarantee proper operation, resistors are often used to pull up or pull down the control lines so they are guaranteed to have a safe, valid, state at all times. A circuit fault which opens the circuit on one of these resistors could result in an indeterminate state of the control line. Each control line must be assessed to determine if this creates an SPF that could contribute to our primary fault definition. If so, a secondary backup resistor or alternative safety mechanism should be employed to remove the SPF. An alternative strategy, for example, would be to immobilize the circuit board such that mechanical stresses are unlikely to cause a circuit to open. Thermal stress or cycling is another contributing factor to PCB trace failure. Isolating the PCB both thermally and mechanically is the surest methodology for preventing PCB failure.

Module/Channel Identification

In most systems, each firing module has some form of unique identifier such that the master controller (and the pyrotechnician) can effectively differentiate exactly which output channel is to fire. Faults where the communications channel is corrupted and mis-identifies a module or channel is dealt with above. In some systems, it is allowed that multiple modules may have the same identifier and fire in concert – when one output is instructed to fire, all modules with that identifier will fire. The problem arises in the field when operators are allowed to set the IDs on the devices. If two modules are given the same ID in error, there needs to be a detection mechanism in place to identify and correct such an error, or all modules must have a unique ID of some kind.

Firing Power Supply Isolation

In some systems, a bank of capacitors are used to store the high energies used to ignite the e-matches. Often, these systems use a step-up or boost converter to take the available system or battery power, and boost it to a higher voltage for the firing system power and e-matches. Various topologies exist for this boost function, however most of them employ an inductor coil between the voltage source and the

capacitor storage bank. This coil can leak voltage from the source into the capacitor bank even when the converter is inactive. The voltage leak would be at the same voltage level as the source, but it only takes about 0.25V to fire an e-match. These boost converters, by providing a path to energize the firing system, create SPFs at the output switches.

One type of boost topology, Single Ended Primary Inductance Conversion (SEPIC), properly isolates the input system power from the capacitor bank / firing system power.

RF Communications Coupling

While it is unclear to what extent cell phone or walkie-talkie communications commonly in use during a pyrotechnics show implementation can couple into the wiring, it is another mechanism by which power can couple into E-match wiring and as such should be addressed. Bead inductors should be added into at least one leg of the wiring path to dissipate any high frequency coupling through antenna inductance effects.

Software

Whenever a programmable processor or even programmable logic is employed in a firing system, software errors must be considered as a source of faults that could trigger our primary fault condition. All of the backups and SPF elimination in the hardware are worthless if the software – correctly – instructs the hardware to fire the wrong effect or at the wrong time. In theory, each functional block of the software must be analyzed for single point failure mechanisms just like the hardware. The most common failure mechanism in software is unintentionally entering a segment of code. This can happen because of a number of mechanisms from poor programming practice to power failure scenarios. In point of fact, the mechanisms that initiate this type of error are so numerous and diverse that it is impractical to deal with them from a top-down organization where we would attempt to identify and show from construction that they could not happen. Instead, the simplest mechanism to employ is identical to the hardware scenario – provide interlocks that prohibit operation from a single point of failure. This greatly simplifies the task to A) identifying points of failure that could contribute to our primary failure definition, and B) devise an interlock to satisfy the elimination of the SPF.

To identify the SPF, we simply assume that from one of a myriad of possible scenarios, the code jumps unexpectedly into any series of instructions. For example, in a normal execution sequence, the software would have gone through some kind of sequence with the operator to arm and then initiate firing of a channel. But what would happen if the software jumped to the code series that initiated firing, without going through the previous steps? One of the more common failure scenarios of this type is at a power fluctuation. As power rapidly cycles just in and out of the safe range, some elements of memory upon which the system depends to store knowledge of its current state could be retained while others could be randomly set to 1 or 0 values, resulting in practically any combination of valid and invalid states that the code could then read and misinterpret. In systems where primary power is supplied via external shared networks, this is particularly problematic as glitches and transients traverse the network due to instantaneous power draws of other devices. Local capacitors and energy storage in the device can

alleviate most of these effects, but it's always a question of at what point does the energy volatility of the network advance beyond the ability of the local circuitry to keep up.

In order to alleviate a software SPF, we recommend hardware interlocks. Hardware interlocks provide system states that are independent of the processor or its memory. For example, if the processor must first set a hardware control to energize the firing system, and that must be confirmed before firing, it eliminates the SPF of jumping directly to the firing code. If this did occur, the failure of the first step of the process would be detected, and if the code jumped to just the right instruction between the test and initiating the firing control, the firing system power still would not have been energized.

Another possible software fault is an overrun condition at the end of the show. The modules are processing a script. In some systems, the script can only be the size of the number of shots in the module. In others, channels can be turned On/Off in addition to firing e-match pulses. This makes the size of the firing script unknown. If there is a software fault in denoting / detecting the end of the show, it is possible that uninitialized or random data could be serviced as if it were the script. This, obviously, would lead to our primary fault condition. To alleviate this software SPF, another hardware interlock may be required.

In transferring the firing commands from the PC to the CM to the FM, CRC and error correction codes are adequate to detect if an error has occurred and a bit had changed. Once it is stored on the CM and/or FM, however, it is still recommended that the stored code that is used to fire an output or group of outputs be protected with some form of CRC to detect if a memory error occurs and a bit changes in the firing command before it is executed.

Loss of Positive Control

In wired systems, positive control is achieved via the hard cabled connection between the master controller and the firing modules, or between the power system (battery or external power) and the master controller. If something goes terribly wrong, one can always pull the plug or yank the cable. Once the cable is pulled, the slaves are dead.

In wireless systems, this type of positive control is not available. One can hit an abort button and cause the RF system to instruct all modules to shut down, but what if the RF system itself is compromised or the controller itself is disabled? Under this scenario, even though the system may be firing all of the right shells in the right place at the right time, the operator has lost positive control and cannot react to unplanned occurrences such as an actor walking too close to an effect at the wrong time or a spectator unexpectedly entering the firing area. Without positive control of the system, these types of errors could meet our primary failure definition.

Secondary Failures

Other failure mechanisms which pertain to loss of accuracy or failure to fire, while not directly related to our primary failure definition, should also be considered as it pertains to the usability and marketability of any firing system. The safest system is one you never use. That said, the objective of this

development is to create a system that satisfies all of the requirements of a simple, effective, and reliable pyrotechnics system which meets all of the safety criteria enumerated above.

Permanent vs. Temporary Installation

In some ways, permanent installations are the simplest scenario. The number of modules and their capabilities are known in advance, they are most often wired, and they can be structured to remove many sources of failure. Temporary installations are by their very nature transient and subject to the harshest environmental conditions. The restrictions on use that make permanent installations simple and affordable make them less than optimal in temporary use, and vice-versa.

Wired vs. Wireless

Wired systems have been the overall mainstay in the industry for the last couple of decades. These days, however, almost every system has a wireless option. Wireless has been tried a number of times of the years, and each time has been ultimately abandoned because it is just too unreliable in under true field conditions. Wired systems are fine for permanent installations, but have their restrictions to which the choreography of the show must be adapted, and restrictions as to the number of modules that can be addressed most often because of power and transmission protocol restrictions.

Most systems currently available employ a Master-Slave architecture. This means that the master controller in the pyrotechnican's hands knows everything about the show and transmits commands to slave firing modules that tells them to fire. One restriction of this architecture is the speed of the communications channel. Because a command goes out from the Master to the Slave to fire a single given output channel, it is not possible to fire two things at the same time. One cannot fire anything, anywhere, anytime, and the choreography must be limited or compromised for this effect. For one or two effects this is not usually noticeable by the general audience, but is noticeable as a ripple effect when a long line or wall of effects is attempted to be fired at the same time. It is also quite noticeable when only two shells are fired, and they always break 1/10 of a second apart. Another drawback of this architecture is the power requirement of the slaves. In most cases the number of slaves is limited to how many can be serviced over the common power network. In some cases power "boost" devices can be added to the network at the cost of higher complexity and lower overall reliability. Large gauge wire may be required for wiring large collections of modules. A wired network, however, is the most robust and least likely to fail.

The most significant drawback to the Master-Slave architecture, however, becomes evidenced when wireless communication links replace the robust wiring. ***All wireless communications systems are fundamentally unreliable [3].*** This is due to two factors that are true of all wireless systems:

A) Wireless packet transmission systems work like eMail – it doesn't matter ***when*** the packet gets to its destination, as long as it gets there. In pyro applications, the ***when*** matters.
B) Physics 101: Any object larger than the antenna will block and reflect the RF signal. This is referred to as a shadow. Shadows can be cast by light posts, rocks, structures, hills, vehicles, and people. The problem is the shadows can move, and there's no obvious way you can know where the shadows are until the show is set up and it doesn't work.

Strangely enough, permanent installations are most suitable for wireless networks, because the variables that make it unreliable in the field are manageable and invariant. Temporary installations, while better served by wired networks because of their reliability, are more troublesome and labor intensive due to wires. Sometimes it's nearly impossible to get a wire where you need it to go, so again the show integrity is compromised for the firing system's weaknesses.

Adding fundamentally unreliable wireless connectivity into the critical path of Master-Slave communications is the worst of both worlds.

Graceful Degradation

As mentioned above, when power for the system is provided by a distribution network the network limits the system, and more importantly if the wired system fails the system fails catastrophically. In a closed loop system, a single wire break can be compensated for and a double wire break only takes out the units between the two breaks. In an open, daisy-chain, or star network, all modules downstream from the failure, which is potentially all modules, fail if the wire is broken or power fails.

Jamming

While all of the above conditions are simply faults that can occur, we must also be cognizant of the possibility of malicious intent being directed at the system. How encryption keys are transmitted and distributed must be considered in order to prevent unauthorized access to the control transmission stream. Physical access to the system by unauthorized individuals must be considered. Jamming devices, while effective over very short distances, can cause a loss of positive control, but cannot in themselves cause inadvertent firing.

References

[1] Datasheet Omron G7SA http://www.omega.com/temperature/z/pdf/z131-148.pdf
[2] "Intrinsic Safety Circuit Design", Paul S. Babiarz http://www.omega.com/temperature/z/pdf/z131-148.pdf
[3] "Wireless Pyrotechnic Firing Systems Operational Reliability in World Wide Environments", Dan Barker and Ken Schroyer, International Symposium on Fireworks 2005 Shiga Japan.
[4]"Wireless Fundamentals", D. Russell and J.L. Mattingly, International Symposium on Fireworks 2005 Shiga Japan.
[5]"Operation of Distributed Radio Networks in Pyrotechnic Environments", D. Russell and J.L. Mattingly, International Symposium on Fireworks 2006 Berlin, Germany.
[6]"Topics on Firing System Safety and Regulations", D. Russell and J.L. Mattingly, International Symposium on Fireworks 2007, Montreal Canada.

Safety Checklist

- Firing circuits are switched at both power and ground.
- Firing circuits shunted between power and ground
- Firing circuits shunted at the capacitor bank (input to firing switches).
- Circuitry is thermally and electrically isolated from the case.
- Interlocks and Detection circuits allow detection of Driver Stuck On failure before firing.
- Intelligent Switches prevent control glitches on firing circuits.
- Double Pull-downs on switch control lines prevent open circuit SPF.
- Continuity Test
    - Separate power supply and path.
    - Intrinsically Safe (No SPF) design.
    - Multiplexed testing limits total current path to safe levels.
    - Detect partial failure of continuity test safety circuitry.
- On-board power system with wired backup prevents communications ringing, allows for graceful degradation, backup in the case of wire break.
- Keyed access and unique ID encryption keys prevent unauthorized access.
- Transmission packets with CRC and encryption make the probability of random interference or tampering vanishingly small.
- On-board clock masters with time code comparison and intelligent jump logic make the probability of timing errors vanishingly small.
- Module IDs are always unique
- Capacitor Bank power is isolated from primary supply by SEPIC boost converter.
- Software/Hardware interlocks remove software SPFs.
- Heartbeat signal provides synchronization and shutdown in the case of LOPC.
- No Relays
- Separation of applied power and control signals

Appendix A

Fault Tree Analysis

Available Upon Request

Appendix B

How to follow NFPA 1126 - Use of Pyrotechnics before a Proximate Audience - and get hurt anyway

by David Crater PE, LumenEssence

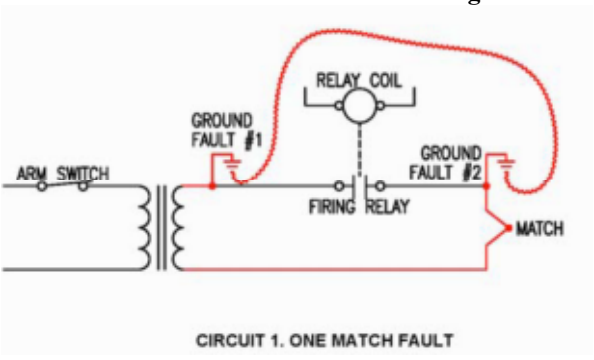
David Crater PE is a principal with LumenEssence, providing consulting and turn-key design for show systems. LumenEssence has designed numerous systems for controlling all aspects of show systems including pyrotechnics, flames, mechanics, audio, video and film effects with installations at major (and minor) attractions worldwide. He can be contacted at: mail@LumenEssence.com.

Imagine standing on your mark, waiting for your cue when, at the expected moment, there is a blinding flash, a deafening roar, and then… nothing. Or maybe it just gives you a scare and provides a story for later. In either case, an unintended pyro ignition can be bad news for actors, for pyrotechnicians, for system designers and for all involved. Aren't there rules or standards to prevent pyrotechnic tragedies? There are, but you can't always count on them to keep you safe, even when they are well intentioned. The National Fire Protection Association (NFPA) has aided in the safe presentation of pyrotechnics since 1978 by publishing and administering two standards for pyrotechnics: NFPA 1123 - Code for Fireworks Display, and NFPA 1126 - Standard for the Use of Pyrotechnics before a Proximate Audience. System designers and industry professionals contribute their expertise in a consensus process to regularly update these standards to reflect continually evolving technologies, products and practices. Any standards process inevitably lags behind current practice by some amount. It takes time to poll members, present issues, invite discussion, and arrive at and publish a final standard. Due to this lag shortcomings in the standards may be identified and may persist for some time before being corrected in a future revision. As a result, an unsafe system may still comply with applicable standards. Experience with the design and use of electric match ignition systems has identified just such a potentially hazardous fault mode which can occur in systems compliant with NFPA 1123 and NFPA 1126.

What is the Problem?

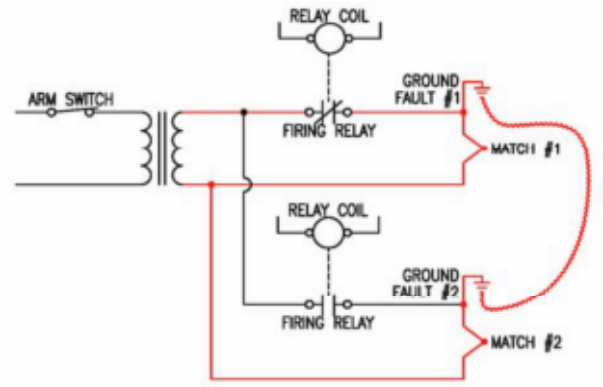
The fault mode in question is characterized by unintended ignition of a shell or other pyrotechnic device connected to an electric firing system. The cause of these ignitions is multiple undetected ground faults in the electric match firing circuitry. Typically, but not always, these faults are in the wiring from the firing system modules to the electric matches. Unfortunately, although both NFPA 1123 and 1126 address the topic of electric firing systems, neither standard contains requirements that would prevent these potentially serious faults. Any unintended ignition of pyrotechnics can be hazardous, but, if while in the vicinity of pyrotechnics, actors or other personnel involved in a presentation rely on the firing system to prevent ignitions, an unintended ignition could cause serious injury or worse.

How Ground Faults Cause Unintended Ignition



CIRCUIT 1. ONE MATCH FAULT

Just as the hazard we are examining is characterized as an unintended ignition, ground faults are an unintended connection of a portion of a circuit to ground, or earth, or any other conductive structure, surface or material. When this happens, and it can and does easily happen, electrical current flows where it isn't supposed to. If two ground faults happen, electrical current can flow from the point of one fault to the other, with possible nasty consequences. Circuit 1 shows how two ground faults can cause an unintended ignition in a single electric match system by allowing current to flow from one ground fault to another, bypassing the firing relay contact intended to prevent ignition until commanded closed. Circuit 2 shows how two ground faults can cause an unintended ignition in a multiple match system.



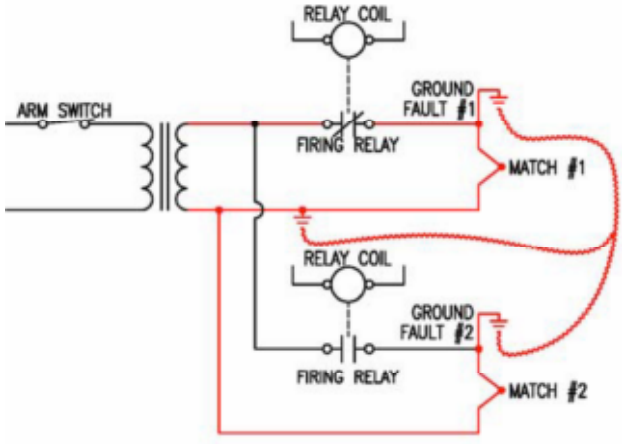
CIRCUIT 2. TWO MATCH FAULT

Bad Luck or Inevitable?

What are the chances of a system developing the necessary two ground faults at the right place at the right time to cause an unintended ignition? As it turns out, the chances are high that this condition can develop. Ground faults can be easily caused by abrasion of insulated wire on exposed metal surfaces, corners, or concrete. The widespread use of inexpensive "zip" cord and temporary wiring in fireworks displays contributes to the hazard. Faults that are acceptable in a system governed by NFPA 1123, where personnel are cleared from the firing and fallout areas before ignition, can become hazards in a system operating under NFPA 1126. Many pyrotechnicians have personally witnessed misfires and unintended ignitions that go unexplained partly because they are transient conditions and partly because temporary systems are dismantled, making diagnosis impossible. In a permanent installation, or even limited engagement system, there is far greater opportunity for the development of faults; traffic between and during shows increases wear on system components and produces faults; degradation over time inevitably leads to faults; entropy prevails. The standard of care in the effects industry includes the statement that "A fault that can go undetected must be assumed to have already occurred." The reason for this statement is that over time faults will accumulate in a system. Although a system may work perfectly when installed, as the faults accumulate eventually two or more faults combine to produce a hazardous or tragic event. In the history of engineering failures, it is most often these multiple fault scenarios that are responsible for tragedies.

Prevention

If we accept the fact that ground faults can cause unintended ignition, as has been demonstrated convincingly in tests and by cooperating spontaneous ground faults in pyrotechnic installations, what can be done to prevent this hazard?

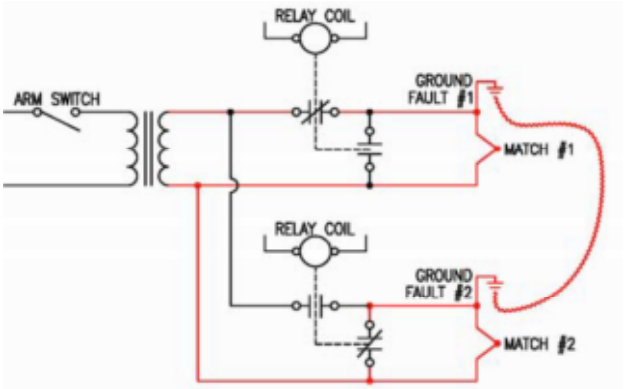


CIRCUIT 3. TWO MATCH FAULT-GROUNDED SUPPLY

What about isolation?

Isolation sounds like a good way to prevent unintended ignition. In fact, isolation is mentioned in both NFPA 1123 and 1126. In NFPA 1126 (2001), paragraph 6.3.2 states: "Power sources used for firing pyrotechnic devices shall be restricted to batteries or isolated power supplies used for firing purposes only." NFPA 1123 has a similar paragraph. Both further state that a transformer is an acceptable means of isolation. Transformers are commonly used in electrical systems for their ability to provide isolation between subsystems. However, in neither standard is there any reference to the purpose for using power source isolation or transformers. Interestingly, we have already proved the case that isolation doesn't work in preventing unintended ignition due to ground faults. Look back at Circuit 1 and Circuit 2. Each circuit represents the power source as a transformer-isolated source. Isolation didn't help; the offending ground faults occur after the isolation. In fact, an argument can be made that a non-isolated, grounded power source would be safer, but that would distract us from the problem of the niggling ground faults. Isolation does have some possible benefits as to reliability, induced currents, and protection from shoot-through of high voltages, but these are complex scenarios that still don't support a conclusion that isolation is always the best approach to ignition source design. Finally, there is the problem that unless we monitor to insure the continued integrity of the isolation, we can't count on it to be there when we need it. For our current concern we have to conclude that ignition power source isolation has no beneficial effect on system safety as regards ground faults.

What about grounding?



CIRCUIT 4. UNINTENTIONAL IGNITION OF A SHUNTED MATCH

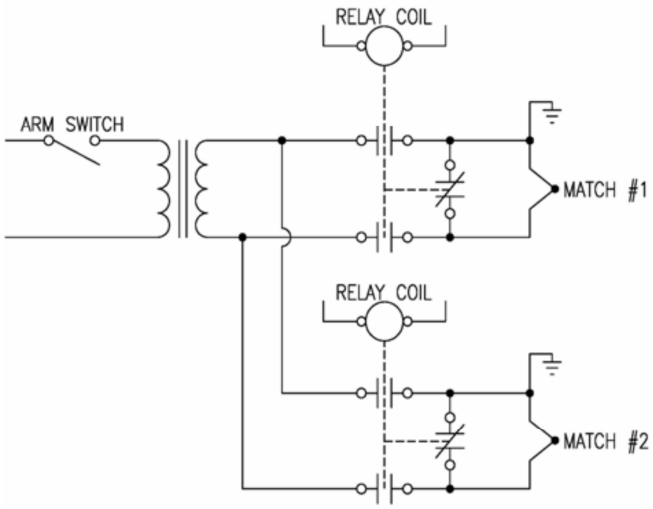
Grounding is frequently cited as an essential component of safe and reliable electrical system design. Can grounding solve the problem of unintended ignition due to ground faults? It could, if we carefully controlled every wire size, length, power supply size, match ignition current, fuse, etc. Circuit 3 shows the same two-match fault as Circuit 2 but with one side of the firing system grounded. Ideally, all the current would go from Ground Fault #1 over to the system ground, bypassing Match #1 and Match #2. In practice however, the current will split among all available paths with some passing through Match #1, some through Match #2 and some straight to the system ground. This reduces the probability of an unintended ignition and increases the probability of a misfire (Match #1 may not fire when commanded) but cannot be relied upon to make the system safe. Usually, grounded systems rely on the ground fault to produce a high enough current to trip a circuit protective device such as a fuse or circuit breaker, preventing all further current flow (in our case, stopping some portion of the show). Grounding does have other benefits relating to reduction of shock potential, dissipation of induced currents, and ease of troubleshooting and diagnostic self-tests. It does not however, solve our ground fault problem.

What about Shunts?

Shunting the match should prevent any current from passing through the shunted match. But, typical electric match resistance is 1.6 Ω. In practice, a few feet of wire, a few terminations, and a relay contact can easily approach 1.6 Ω. Because of this, the shunt is not perfect and the current is split between the shunt and the match. Circuit 4 shows an example of a shunted match receiving current due to ground faults. Once again, the precaution improves performance, but is not an adequate guarantee of safety.

What about GFCIs?

Aren't they designed to detect and protect against ground faults? Interestingly, GFCI stands for Ground Fault Circuit Interrupter, and sounds like the right animal for us. GFCIs detect "missing" current by comparing the current in both legs of the power source circuit; if the two currents aren't equal some must have been "lost" to another path, usually a ground fault. On detecting this condition GFCIs interrupt the circuit (once again stopping some portion of the show). The first limitation of a GFCI is that it cannot do its job if it is installed before an isolation transformer. The second limitation is that in order to perform this detection GFCIs require a ground connection and this connection must be after any isolation device, contrary to the current code's requirement. In theory this will solve our problem.



CIRCUIT 5. SAFE FIRING CIRCUIT

In practice, large distributed systems with many matches frequently have many low current ground faults or leakage paths. If the sum of all leakage paths approaches the current for a single match, the GFCI cannot distinguish between multiple harmless leaks or a single significant leak. This defeats the GFCI and results in nuisance tripping.

Design of a safe system

Fortunately for system designers, pyrotechnicians, and other personnel needing protection from unintended ignition, there is a viable solution to achieve a safe electric firing system. Ironically, the solution is described in NFPA 1126, but only in the appendix where it is relegated to "informational" status instead of the "requirement" status accorded the body of the standard. Paragraph A.6.3.3 states: "Firing circuit design should be such that neither

igniter lead is electrically connected to the firing power source until ignition is intended. It should not be permitted to wire one side of multiple match terminals together, then to switch current to the other terminal of the igniter." Another item from the appendix introduces another widely used (but not required!) safety element. Paragraph A.6.3 states in part:
"Electromagnetic induced currents in firing circuit wiring can be reduced by utilizing one or more of the following methods: … (4) Shunting near the electric match" Finally, the body of the standard states clearly in paragraph 6.3.3 that: "All firing systems shall be designed to ensure against accidental firing by providing at least a two-step interlock in which no firing power can be applied to any firing circuit unless the operator intentionally does both of the following: (1) Enables or arms the firing system and (2) Deliberately applies firing power" Circuit 5 shows a design incorporating all of the above requirements and recommendations as well as the previously discussed, but dubious, power source isolation. The features of this design include: separate arming switch, supply isolation, individual firing command control of each match circuit, dual-leg match isolation, and match shunts. The essential feature of this design is the use of dual contacts to interrupt both sides of the match leads. This is what prevents those pesky ground faults from rendering the ignition system unsafe. (Note that while the schematic and text suppose the use of a relay, interruption of both sides of the match lead can equally well be accomplished by a solid state device such as a FET.)

Understanding Standards
Standards are not a substitute for common sense or engineering analysis. Even the NFPA recognizes this. In the "Important Notice About This Document" in NFPA 1126 it states: "..the NFPA … does not … verify the accuracy of any information or the soundness of any judgments contained in its codes and standards." And: "Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances." Standards can be an obstacle to good system design. Ideally, standards are a mechanism for lay individuals to benefit from the experience of acknowledged experts (the standards' authors) without having to understand the underlying technical details. When a standard omits requirements to address known unsafe conditions, such as our ground faults, a false sense of security is created which can lead to tragedy. Similarly, standards can impede improved system designs; as we have seen, the requirement in NFPA 1123 and 1126 for "isolated" power sources is of questionable value and may prevent superior designs that could benefit from the use of grounded distribution systems. It may be difficult or impossible to obtain a variance from the authority having jurisdiction to allow the use of such an improved design. The NFPA developed two pyrotechnic standards to serve the needs of two types of pyrotechnic presenters. For a special events pyrotechnic systems engineer NFPA 1123 is typically the applicable standard. It dictates mostly sound practices which can be demonstrated to be safe because, and only because, the entire firing field and fallout area will be cleared of personnel before bringing the ignition power source anywhere near the ignition system. For these events there are two overriding principles: (1) The show MUST go on; given the special event nature of many shows, anything that would delay or interrupt the show seriously diminishes the event. Minor flaws (such as unintended second ignitions or misfires) are not significant. (2) The primary safety tactic: Clear the entire firing field and fallout area of personnel before bringing the ignition power source anywhere near the ignition system. For a show systems engineer dealing with personnel in proximity to hazardous effects, NFPA 1126 is typically applicable but falls below the required standard of care with regard to the prevention of unintended ignition. To implement only the requirements of NFPA 1126 would be negligent because such a system IS NOT SAFE when personnel are in proximity to the effects. For these types of shows two different overriding principles apply: (1) The safety of persons is PARAMOUNT; all potentially hazardous effects systems, including pyro, must be designed in a manner which does not allow undetected faults to cause a hazardous condition. (2) A hazardous condition must be remedied even if it causes delay or forfeiture of all or portions of the show.

The Next Steps
After all is said and done there are two implications for NFPA 1126. First, electric match ignition systems that rely on single pole firing relays are not safe for use in situations where personnel are in proximity to the effects after the ignition power source is present in the system. The standard already recognizes this issue as indicated by the inclusion of paragraph A.6.3.3 wherein dual-leg match isolation is recommended. Hopefully, as the standards committee and industry professionals become aware of the potential for harm if this recommendation is not followed, the standard will be revised to require this practice. Second, isolation of ignition sources as described in NFPA 1123 (2000) and 1126 (2001) is inadequately described. The benefits of isolation, if any, need to be described and coordinated with provisions for designs with grounded distribution systems. This will allow designers to continue to improve the safety of electric ignition systems.