Protecting the Optical Network
Ram Oron, Ph.D., KiloLambda Technologies

As optical powers in fibers increase — and fiber networks are spread — network safety is becoming an area of concern.

Advanced optical networks are widely spread; an increasing number of them are "all optical" and not only point-to-point lines, in which all inputs and outputs are controlled. This situation raises new issues that should be considered. First, power can be aggregated from many sources, which are neither always predictable nor centrally controlled. Second, damage to a single component can jeopardize the whole network operation.

![Figure 1. Damaged Core in a Fiber Connector](image)

The need for higher bandwidth in optical communication systems pushes optical powers up. For example, 32 channels, each having power of 10 dBm (10mW), leads to a total power of approximately 25 dBm (0.3W) in a single-mode fiber. Standard powers in today's optical networks are as high as 27 dBm (0.5W). Thus, optical components in systems must withstand these high powers. In addition, these high powers require high power amplifiers, such as Erbium doped fiber amplifiers (EDFAs) and Raman amplifiers. This should also be of concern, as such amplifiers may often have high power spikes and additional high pump powers. Both the network properties and the high powers present in the networks call for damage preventing solutions in optical networks.

Laser Damage

The study of laser damage to optical materials is a subject of major interest since the invention of the laser in the early 1960's. Until recent years, the study was mainly concerned with bulk materials and not with fibers. However, with the increasing powers in optical fibers, it has many relevant results applicable to fibers today. For example, a 30 dBm (1W) of optical power in a standard single-mode fiber, having a mode field diameter (MFD) of approximately 10 microns, has a power density of 1MW/cm² in the fiber core. This value of CW or repetitive pulse power density is in the range of damaging bulk optical materials.
Figure 2. Image of a SMF after Fiber-Fuse

A damaged core in fiber connectors is quite a well-known phenomenon. This usually occurs when the connector end-face is not cleaned properly, even at moderate powers. An example of such a damaged core is shown in Figure 1. Evidently, such connectors need to be replaced. Other sensitive points are optical coatings (such as anti-reflective or absorbing coatings), defects, scratches or contamination of surfaces, fiber splices and connectors. Damage to these mostly results in damaged optical surfaces or connectors. Avoiding such damage, and the design of high power components was the subject of recent research. Some steps were suggested; these include better handling of the fibers and components — namely, cleanliness and defect-free manufacturing of optical coatings; and great care in processes such as polishing and cleaning, avoiding fiber bends and screening for the best components. These steps are of course essential and good practice; they improve the power handling of components. However, they provide only a partial solution to high power network protection, as even well-handled components will eventually be damaged at some power level. As opposed to the external damage mechanisms described above, which mostly occur on surfaces, a much more dramatic damage may occur to the fiber core, namely, fusion of the core or "Fiber Fuse".

The Fiber-Fuse Phenomenon

Fiber Fuse is a phenomenon in which the core of the optical fiber is destroyed [2-4]. It has been known for more than 15 years, but only in recent years — as the powers in optical fibers increased — has it become a concern in fiber communication systems. The exact mechanism of the phenomenon is still debatable, and involves either a thermal shock model [2] or a Rayleigh instability [4]. In any case, the damage is generally initiated by contact to the fiber end from splices, internal gratings, or other defects. The damage propagates at speeds on the order of one meter per second towards the power source, and looks from the outside as a bright light spot propagating inside the fiber. The damage can propagate through splices and connectors, and can destroy several kilometers of fiber, as long as the power is on. In single-mode fibers, the phenomenon can start at power range as low as 30 dBm (1W), and the higher the power, the more likely the phenomenon is to initiate.
Figure 3. Protected Ring Network Scheme

The core of a fiber subjected to the fiber fuse phenomenon is destroyed; it no longer transmits light, and the damage appears as bubbles along the core's length. An image of such a fiber is shown in Figure 2. The phenomenon was observed in SMF and other fibers, and found out to be a common problem to all, albeit with different threshold powers. The damage from the fiber fuse phenomenon is different than others; it is not located in a single isolated point, and can harm many components along the way. Moreover, the fiber itself should be replaced. Also, the damage will initiate from some unknown weak point in the network (splice, contaminated connector, etc.) and the initiation of the fiber fuse requires only a high power optical source (laser, amplifier, or accumulated sources). One can therefore conclude that fiber fuse is a threat to optical networks.

Making the Network Safe

Networks are complex system, and every type of network requires specific protection solutions, beyond the general protection of components. In electrical systems, various types of fuses protect against over-current. Wireless communication systems use frequency hopping and gain regulation to avoid both damage and communication interruption. Computer networks are protected against harmful data (viruses) by firewalls, which involve both software and hardware.
The methodology used in most of these networks involves the division of the network to protected (safe) and unprotected zones. In the protected zones, the conditions (such as power level, type of data, or electrical power) are regulated, thus reducing or eliminating the chance of a mishap. The protected zone is separated from the unprotected zone by special protection devices, such as firewalls or fuses. (Note that a similar method is generally used in physical security, such as in airports.)

Different protection devices are generally applied to different parts of the networks. These depend on their importance, vulnerability, and whether the damaging phenomenon is intentional or unintentional. Also, specific protection devices could be added inside the protected zone, for example, next to high power sources.

Adapting this methodology to optical fiber networks requires two main things: First, defining which specific protection devices or tools can be used. Second, mapping the network, and suggesting the locations for the protection devices.

Possible tools for protection against over-power in optical networks are optical switches (or fuses), power limiters, and fast control loops. The switches and limiters can be passive, whereas the control loops are active and thus more complex; also, these control loops sometime require control over the power source, which is not always possible. In addition, as we are often very close to the threshold of the harmful fiber fuse phenomenon — which is quite unique to optical networks — there is a need for a passive high power network protector against it.

Figure 5. Protected Optical Router Scheme

In general, the protecting devices should surround the network's core or vulnerable equipment, in order to avoid external power sources from reaching into them. The next few figures exemplify protection configuration. An example of a protected ring network is shown in Figure 3. Here, the inner ring is the protected zone, whereas protection devices are placed in all input and output ports. Next, Figure 4 provides an example of a protected submarine cable. Here, two protection devices are placed in the ends of the submarine cable. These can prevent damage such as from fiber-fuse, so the submarine cable will not have to be replaced. Figure 5 presents a protected optical router, which is surrounded by protection devices on both input and output lines. In this scheme, any other expensive and vulnerable equipment may replace the optical router. Other protection schemes are of course possible.

In conclusion, optical networks are nowadays susceptible to serious damage by over-power. For every network, the protection solution is a combination of the protecting devices used, and the architecture in which they are placed. Deploying any protection scheme requires the use of fast, passive building blocks like optical switches (or fuses), power limiters, and network protectors against the fiber fuse phenomenon.
References

Ram Oron, Ph.D., is the CTO of KiloLambda Technologies (Tel-Aviv, Israel; www.kilolambda.com). E-mail the author at: ramoron@kilolambda.com.