

Protection Architectures for WDM Optical Fibre Bus Sensor Arrays

Eduardo López Izquierdo, duduyuhu@yahoo.es

Paul Urquhart, Paul.Urquhart@unavarra.es

Manuel López-Amo, mla@unavarra.es

Universidad Pública de Navarra, Spain

Abstract

We propose and critically compare novel designs of wavelength multiplexed fibre sensor networks that can withstand one or more cable failures. Our designs use protection switching to recover service and they can be based on four combinations of dedicated, shared, line and path protection. We identify architectures that can (1) tolerate at least one failure at any point, (2) perform signalling without requiring additional external resources and (3) impose nominally equal transmission impairments on all channels, be they in the working or protection states. Our preference for most circumstances is the “direct unidirectional sensor array”, operated by either dedicated line or dedicated path protection.

1. Introduction

The increasing dependence on telecommunications services has created a need for optical fibre networks that are not disrupted in the event of accidental damage to cables by natural disasters or human activities [1]. To this end, wide area and metropolitan networks are now usually configured as self-healing rings and other designs with redundancy that use “protection” to regain service in the event of cable failure [2 – 4].

Another application for optical fibre networks is the multiplexing of optical fibre sensors [5]. The uses are diverse, including monitoring the physical integrity of buildings, bridges, dams and pipelines and the surveillance of transport networks, manufacturing plants, power stations and other large installations. However, in comparison with telecommunications networks, few studies have been published on multiplexed fibre sensor arrays that are designed to continue service in the event of unintended cable damage [6, 7]. Where the structure being monitored is of high value (oil pipelines, power transmission lines, etc.), human safety is at risk (bridges, dams, chemical storage sites, nuclear plants, etc.) or perimeter security is a concern (airports, banks, etc.) [8] the continued operation of the sensor network after accidental or malicious damage is of increasing importance.

This paper reports a study which critically appraises novel network architectures for sensors that allow service continuity after one or more cable failures. The networks we study are optical fibre buses based on wavelength division multiplexing (WDM). Bus structures have been widely used for time division multiplexing (TDM), frequency division multiplexing (FDM) and coherence multiplexing [9, 10]. However, fibre Bragg gratings, which are now widely available low cost and low loss wavelength reflectors, have enabled WDM techniques to increase in importance among their competitors. The gratings can act as sensors themselves [8 – 10] or can be used to identify the sensors within the network [11, 12]. In this way WDM bus networks make efficient use of the fibre and enable the multiplexing of intensity or interferometric sensors that respond to many measurands. Therefore, they are not application-specific, which confers cost advantages.

Optical fibre networks that incorporate protection strategies are well known in telecommunications engineering [1 – 3]. However, to our knowledge, this is the first reported classification and appraisal of protection categories and topologies in the context of networks with the prime objective of multiplexing sensors. We report bus architectures that satisfy

three criteria simultaneously: 1. the network must withstand at least one cable failure at any point; 2. it must be possible to signal the failure and the need to take appropriate action to the relevant parts of the network without requiring external resources and 3. the network design must exert nominally equal transmission impairments on all channels, even after responding to a failure. Complying with these requirements simultaneously is very demanding but we show that it is possible with the architectures that we propose. Moreover, some of our designs can survive certain categories of multiple failures.

Our investigation is of architectural principles [4], rather than physical layer performance and it starts in Section 2, which overviews unprotected and partially protected fibre bus ladder networks as multiplexed sensor arrays. We propose a novel protection network in Section 3 and explain how its operation can conform to four categories of protection that are well known in telecommunications engineering. Protection switching is only possible if the network manager can signal the presence of a fault and request appropriate remedial actions [13]. The signalling requirements of bus networks are summarised in Section 4. Section 5 describes in detail how our main topology responds to cable failure, making reference to the four categories of protection and in each case describing the signalling actions. Section 6 overviews three alternative topologies and explains the circumstances in which they can withstand multiple failures. In concluding, Section 7 argues for our preferred strategies for topologies and protection categories.

2. Unprotected and Partially Protected Bus Networks

A dual fibre bus network for multiplexing an array of N sensors is shown in Fig. 1 and it is the basis for the others in this paper. It is not measurand specific and so it has a wide number of applications, according to the sensors selected. The sensors are designated S_i (where $1 \leq i \leq N$) and each one is accompanied within a sensor unit SU_i by a fibre Bragg grating that reflects a narrow bandwidth centred at wavelength λ_i . The S_i perform the modulations in response to the required environmental influence, while each grating uniquely identifies its associated sensor and so it is essential for WDM operation of the network. The lasers at the transmitter node (TN) are usually unmodulated but have a bandwidth that is sufficiently broad to raise the threshold power for stimulated Brillouin scattering in the transmission fibre [14]. (Alternatively, they can be narrow band with an imposed modulation for the same purpose.)

Figure 1 shows a distribution fibre and an aggregation fibre. There are broadband couplers along the length of each of them and so there is no wavelength discrimination. Launched waves from the TN are transmitted to all of the sensors and, in the configuration shown in the top of Fig. 1, light of wavelength λ_i only is reflected by the grating at sensor unit SU_i and makes a return pass through sensor S_i . From there it is coupled on to the aggregation fibre and to the receiver node (RN), together with the other wavelengths [12].

For sake of completeness, the lower portion of Fig. 1 shows an alternative location for the sensor so that it is physically separated from the fibre Bragg grating. Then the signal makes only a single pass through the sensor, which has three consequences: double modulation by S_i is eliminated, the induced transmission loss due to S_i is halved and no reflected signal travels back to the TN. The desirability of these attributes is application specific. Figure 1 shows a further pair of optional features, marked OTDR-D and OTDR-A, which are optical time domain reflectometers [15] on the distribution and aggregation fibres, respectively. By transmitting and receiving pulses at out of band wavelengths, they allow the integrity of the network to be monitored and the location of any fibre fracture to be estimated.

Inspection of Fig. 1 reveals that, in travelling from the TN to the RN, all channels encounter the same number of broadband couplers and transit the same total number of spans of distribution plus aggregation fibre between the couplers. Consequently, they all experience similar propagation delays and impairments due to loss, dispersion, non-linear effects and accumulated noise. No channel is systematically favoured or disadvantaged. Physical design studies of bus networks predict optimal performance when the splitting ratio of the couplers is about 5 – 10% (but the precise value is not of concern in this paper) [16, 17]. When the network has around ten sensors or fewer, the total loss may be acceptable to

achieve the required operating signal to noise ratio [16, 18]. However, amplification is required for operation with a larger number. Various schemes have been proposed for bus networks, including discrete and distributed erbium doped fibre amplifiers and fibre Raman amplifiers [11, 12, 18, 19] but the details are not of direct relevance here.

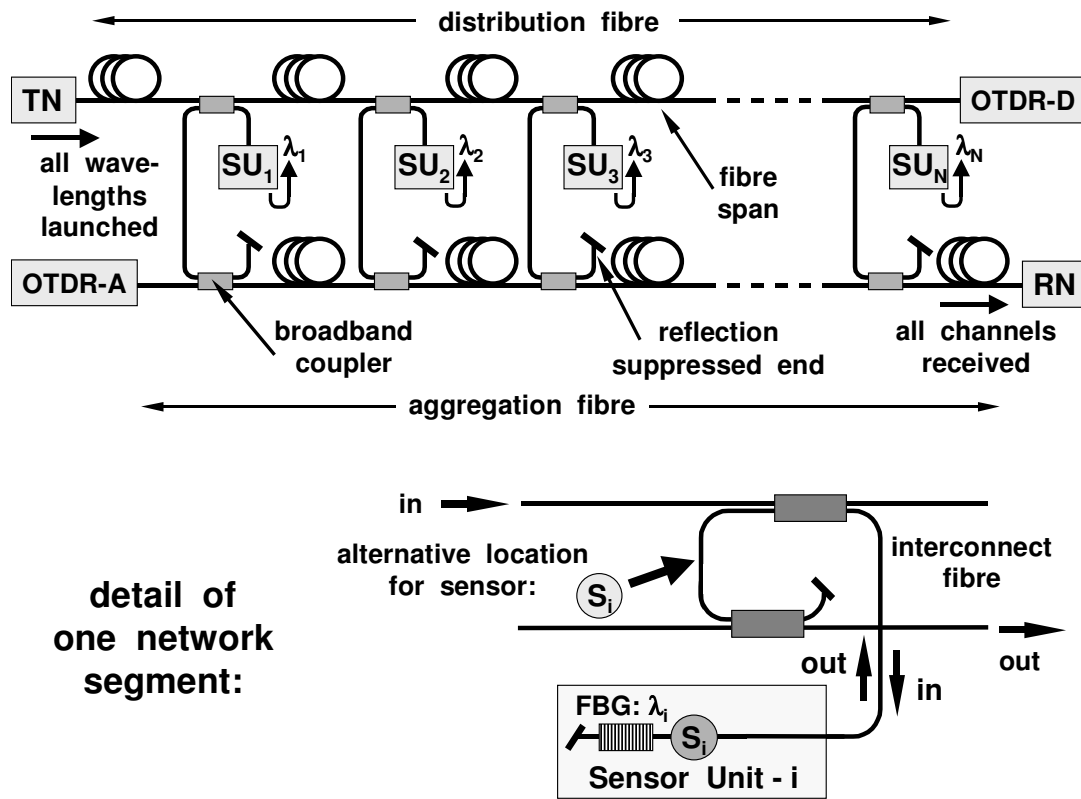


Figure 1 Top: Fibre ladder bus network for the multiplexing of optical sensors. Bottom: Detail of one of the network segments drawn differently. TN = transmitter node, RN = receiver node, SU_i = sensor unit i , S_i = sensor i , FBG = fibre Bragg grating. OTDR-D and OTDR-A = optical time domain reflectometers in the distribution and aggregation fibres (optional).

The distribution and aggregation fibres are shown in Fig. 1 without reference to how they are contained within cables. There are two main options. The first is lower cost, in which they are in one common cable, but it is totally unprotected. If the cable is cut at any point, there is complete network failure because all signals must pass through the entire length of the cable; part being by the distribution fibre and the remainder by the aggregation fibre. The second option is to cable the distribution and aggregation fibres separately, avoiding co-location at any point along their length. When the distribution fibre is cut, there is a loss of signal (LoS) only from the sensors between the point of failure and the RN, for lack of optical input. Alternatively, when the aggregation fibre is cut, the sensors between the TN and the point of failure no longer have an output path but the others survive. The interconnect fibres that link the various SU_i with the distribution and aggregation fibres (via the couplers) can also be damaged. When this happens, only the affected sensor(s) fail and the rest of the network remains functional.

In some circumstances the partial protection offered by placing the distribution and aggregation fibres in separate cables may have to suffice as a compromise between cost and security of service. Sometimes the strategy can be justified by using more sensors than are strictly necessary for the monitoring function that they perform. The entire cabling could be folded in some manner to ensure a reasonable spatial distribution of functioning sensors when there is a cable cut. Then the redundancy necessary to withstand failure would be in the number of sensors, rather than through duplication of fibres. However, overprovision of sensor units is expensive when it entails extra cable lengths. The longer cable ducts and the

additional amplification to overcome the increased transmission and coupler losses can be costly. Therefore, ensuring continued operation in the event of cable failure requires more advanced bus topologies, as addressed in the following sections.

3. Direct Unidirectional Sensor Array: General Description

The “direct unidirectional sensor array” is our first adaptation of the basic network design, in which the word “unidirectional” refers to signal propagation in the cables between the sensor units, rather than the individual fibres. Figure 2 shows several segments of a bus network with four fibres that are common to all of the sensors. The two fibres at the top of the diagram are co-located the “working cable” and the two at the bottom are in the “protection cable”. Each cable contains one distribution fibre and one aggregation fibre. The fibres that connect the sensors to the working and protection cables are the “working interconnect” and the “protection interconnect” fibres, respectively. The input light to sensor S_i can be carried by the distribution fibres within the working and protection cables, where it is designated W_{in} and P_{in} , as appropriate. Similarly, the modulated outputs from the SU_i are carried by one or both of the aggregation fibres. They are designated W_{out} and P_{out} and are within the working and protection cables, respectively.

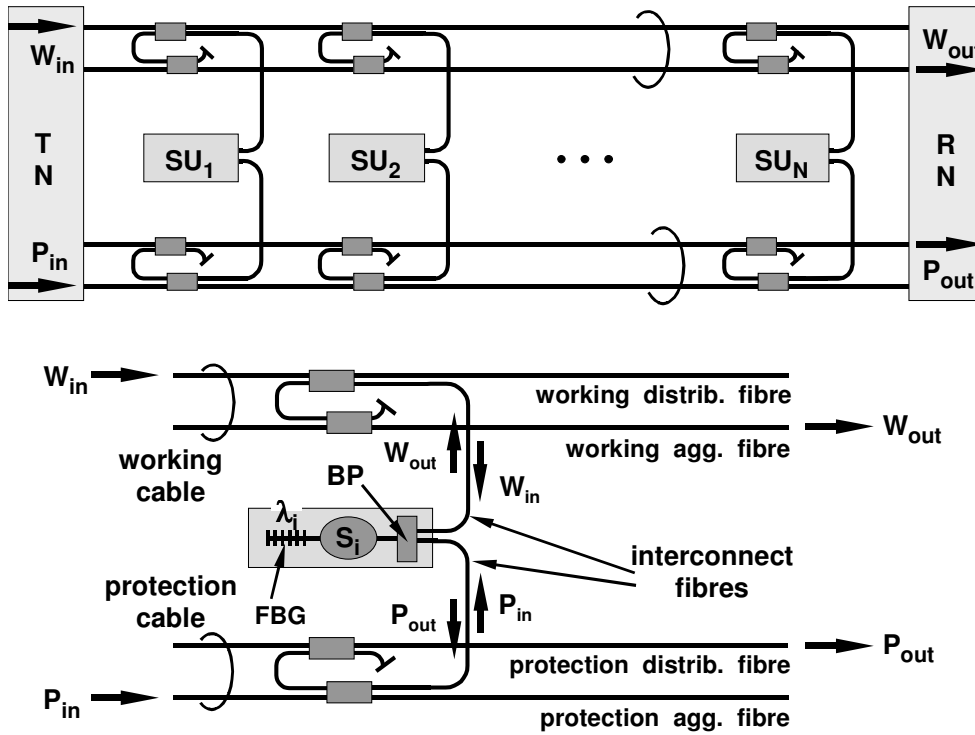


Figure 2 Top: Direct unidirectional sensor array network. Bottom: Detail of one segment. TN = transmitter node, RN = receiver node, BP = branching point, SU_i = sensor unit i , S_i = sensor element i , FBG = fibre Bragg grating. W_{in} and W_{out} = working cable: input and output, respectively. P_{in} and P_{out} = protection cable: input and output, respectively.

In Fig. 2 the total number of spans of fibre through which every channel passes is the same, be it by the working or the protection infrastructure, and so all channels experience nominally equal transmission impairments and propagation delays. Furthermore, the losses caused by the broadband couplers are the same as in the unprotected network of Fig. 1. These are desirable attributes that are not necessarily shared by telecommunications self-healing ring networks [1 – 3]. We have therefore satisfied the third of our criteria of acceptable operation stated in Section 1.

The network design in Fig. 2 does not aim to protect against failure of the TN, RN or any of the SU_i . In common with telecommunications practice, the probability of failure at such

key locations is minimised by duplicating the internal equipment and electrical power supplies. Nevertheless, should one of the SU_i be rendered completely inoperative, all of the others can continue to function, irrespective of the category of protection that is used to ensure the continued transmission by the fibres and we believe that this is an advantage over some designs of ring network.

There are four categories of protection for the network shown in Fig. 2. It can use “dedicated” or “shared” protection and each of these has sub-categories called “path” and “line” protection. (In telecommunications networks dedicated and shared protection are commonly designated “1 + 1” and “1 : 1”, respectively but we do not use this terminology.) We start with the distinction between dedicated and shared protection [1 – 3]. The sensor unit in Fig. 2 contains a component that is not included in Fig. 1, called the branching point (BP), and it can be either a passive 3 dB 1x2 coupler or a 1x2 photonic switch. Dedicated protection requires a coupler, while shared protection requires a switch.

In dedicated protection, the transmissions from the TN are carried by the working distribution fibre to the sensors in normal operation. The modulated wave exiting the sensor is passively split by the 1x2 coupler and then propagates by both of the aggregation fibres via the interconnect fibres. In normal circumstances, the receiver selects the channel W_{out} from the aggregation fibre within the working cable and discards P_{out} . When there is a LoS due to cable failure, the network performs up to three consecutive switching actions in order to restore service. First, the receiver in the RN switches to the aggregation fibre within the protection cable in an attempt to receive P_{out} . If the channel(s) remain undetected, the laser(s) in the TN switch to the distribution fibre within the protection cable and so launch via P_{in} . The RN still attempts to detect P_{out} and if service is not present, there is a last switching action, in which the receiver(s) switch back to the aggregation fibre within the working cable to receive W_{out} .

When shared protection is used the lasers in the TN are connected to the working distribution fibre in normal operation. The 1x2 switch in SU_i selects whether the waves to and from the sensor travel via the working fibres or the protection fibres. Only the working fibres are used in normal operation and only the protection fibres in the event of a cable failure. When a failure occurs, three switches (or groups of switches) have to change position from the working fibres to the protection fibres. They are: (a) at the TN, (b) the 1x2 switch(es) at the sensor unit(s) and (c) at the RN. Automatic protection switching (APS) protocols [20] are required to control the process and upon completing the three switching actions, operation is entirely by the protection fibres.

There are important differences between dedicated and shared protection. The 1x2 couplers used in each SU_i in dedicated protection typically cause a minimum of 6 dB loss (3 dB in each direction) but they are relatively low cost components. In contrast, the 1x2 photonic switches used in shared protection are lower loss but more expensive and require electrical power. In dedicated protection sensor signals always attempt to travel from the SU_i to the RN in both the working and protection cables and the RN accepts either W_{out} or P_{out} , according to which is present. The switching that occurs after LoS is only in the RN and TN. In contrast, in shared protection light is confined exclusively to either the working or the protection cables and it is achieved by the switches at the SU_i throughout the network. Consequently, switch control algorithms are more complicated in shared protection.

There is a facility called “spatial re-use” that can be offered in telecommunications shared protection networks [2, 3]. It could be beneficial if ever the networks described here were used for combined sensing and data services. (A simple example would be to reserve several WDM channels for direct point-to-point data links between the TN and RN and so increase the number of paying customers.) During normal operation, when all cables are perfectly intact, the protection fibres are not in use and so could be loaded with low priority traffic. If there is a break in the working fibre, protection switching occurs and the sensor traffic previously carried by the working cable is re-routed via the protection cable. In that case the low priority traffic is lost. Capacity on the protection cable could be sold by the operators as being at higher risk of failure and priced accordingly. In this way, it would be

possible to recover some of the costs of providing the protection capacity for the high priority traffic. It should be noted that spatial re-use is not available with dedicated protection.

Both dedicated and shared protection networks can operate by what are known as “path” and “line” protection. In path protection each sensor, and its associated wavelength, is protected individually. It is achieved by placing one switch per channel before the wavelength multiplexer at the TN and one switch per channel after the wavelength demultiplexer at the RN. However, in line protection, all sensors and their associated wavelengths are protected and switched by only one request. This means that there is only one switch (serving all channels) at the TN and it is located after the multiplexer. Similarly, there is one switch before the demultiplexer at the RN. Clearly, the greater number of switches in the TN and RN in path protection increases the costs. Similarly, the APS protocols are more demanding. However, as argued in Sections 5 & 6, path protection can offer greater resilience against certain types of multiple failures.

4. Signalling Requirements: General Considerations

In common with telecommunications, the presence of a fibre failure and the subsequent command to activate protection switching must be communicated between the different parts of the network. We refer to these telemetry communications as “signalling” [13, 20] (some authors use “messaging”). Signalling traffic is an integral component of the protection switching procedure and it is high priority because it must not depend upon being carried by the failed fibre. It is low bit rate (if it is digital) or low bandwidth (if it is analogue). Nevertheless, the complexity of both the physical connectivity and the information content for the signalling depend upon the category of protection. In dedicated protection all of the switches are in the RN and TN and the signalling merely requires point-to-point communication between them, which is relatively simple and low cost. However, shared protection architectures employ a switch at each sensor unit, which complicates the signalling connectivity requirements and switch control software. The signalling traffic volumes are greater when the channels are switched individually (path protection) than collectively (line protection).

In telecommunications networks the APS protocols can be either distributed or centralised. Distributed operation usually requires a processor to be placed at the site of each switch. Extrapolating to sensor networks, the intelligence would have to be included in the SU_i , which is likely to be costly and more technically demanding and so we do not consider it further. When the protocols are centralised, the failure detectors and associated processor units are most conveniently located in the RN. The failure detectors are activated by (a) a complete LoS, (b) signal fading below some predefined threshold or (c) an unacceptable signal-to-noise ratio. (Bit error rate measurements are not relevant in analogue sensor networks.) Signalling is then sent to the slave switches in the TN (in all cases) and in the sensor units (in shared protection).

The signalling transmission requirements are dependent upon the network’s physical topology. Figure 3 shows a design that can reduce or even eliminate all signalling outside the end nodes of the network. An experimental demonstration of this network has been reported in Ref. [21]. Figure 3 complies with the connectivity requirements shown in Fig. 2 but the TN and RN are co-located and so it can be said to be a physical ring but a logical bus. The transmitters, receivers and associated switches can all be in the same equipment rack or line card so that signalling between the TN and RN is achieved entirely through electronic circuitry. In that case, no signalling transmissions need exit the TN/RN node enclosure in dedicated protection networks, leading to improvements in costs, network simplicity and reliability. Unfortunately, the suitability of the configuration shown in Fig. 3 depends on the required sites for the SU_i and various geographical constraints. Where the cables are underground, it would often need longer trenches than the linear configuration of Fig. 2, leading to costly civil works. Therefore, sending the signalling between the TN, RN and SU_i may be unavoidable and the means by which this can be achieved are now considered.

Signalling traffic can be carried either by an infrastructure that is in some way physically separate from the sensor network or by the sensor network’s own fibres. Firstly, consider the

physically separate means. One could install separate fibre(s) which are devoted entirely to signalling but it is usually unrealistically expensive. There might sometimes be a data communications network in close proximity to the sensor network and capacity could be bought from the network operator. However, a shared protection strategy would demand interconnecting every sensor unit to the data communications network, which would increase the costs. An alternative means of transmission, such as a radio link, would be much more cost effective and, provided that its failure probability is acceptably low, it could be a viable technical choice, especially for dedicated protection.

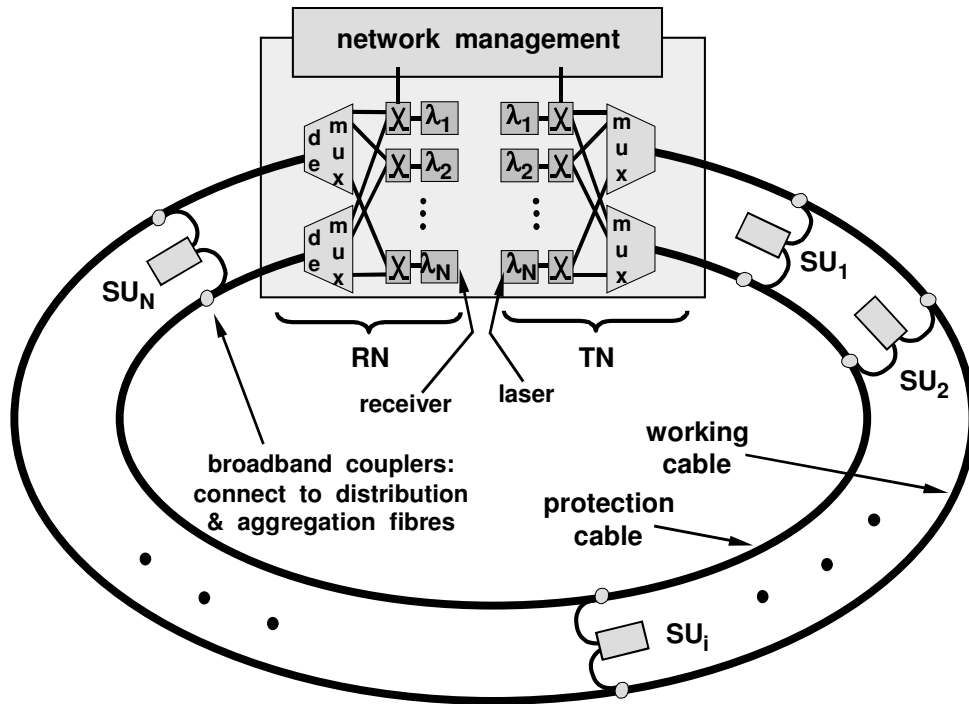


Figure 3 Direct unidirectional sensor array folded to form a physical ring with a co-located transmitter node (TN) and receiver node (RN). Each sensor unit (SU_i) is connected to the distribution and aggregation fibres within each of the working and protection cables. This example is for path protection: each laser and receiver is connected to a 1x2 switch that is controlled by a common network manager.

We turn to the use of the existing fibre infrastructure for signalling. It is a low cost option because no external resources are required and it is the only one that fully satisfies our criteria for acceptable protection schemes stated in Section 1. However, the challenge is to ensure that the signalling traffic is not blocked when a fibre failure occurs. Two choices for the signalling traffic format are to superimpose pilot tones [22] on the existing channels and to devote one WDM channel to signalling. (In contrast to telecommunications practice, such as SDH/Sonet, [2, 3] sensor data is analogue and digital headers cannot be conveniently employed). Pilot tones are analogue over-modulations on each of the channels and they confer the benefit of not requiring dedicated lasers and receivers or occupying additional spectrum within the optical amplifier gain bandwidth. However, they complicate the required signal processing at the receiver and they cannot be used to carry information contra-directionally in a fibre with respect to the sensor data. In contrast, a wavelength λ_s , which is devoted exclusively to telemetry signalling, can often be propagated in the opposite direction to the N sensor channels and this is the strategy that we consider in Sections 5 and 6.

5. Direct Unidirectional Sensor Array: Responses to Failures

The four categories of protection – dedicated line, dedicated path, shared line and shared path – all have particular characteristics, determining the locations and numbers of failures against which they can protect and their signalling requirements. Their operation during cable

failure is now described and Table 1 summarises their main features. The explanations given here refer mainly to Fig. 2.

	Line	Path
Dedicated	<ul style="list-style-type: none"> • Passive Y-couplers in the SU_i • One switch in the RN and one switch in the TN • One interconnect fibre failure causes protection switching of every channel • Simple APS protocol <ul style="list-style-type: none"> – it only communicates between the TN and RN – there is only one alarm condition: switch to the protection cable • Signalling: Use a devoted wavelength counter-propagating on the protection cable 	<ul style="list-style-type: none"> • Passive Y-couplers in the SU_i • N switches in the RN and N switches in the TN • One interconnect fibre failure causes protection switching only in associated channel • One failure in the distribution or aggregation fibres generates N alarms • The APS protocol communicates between the TN and RN but not the SU_i for each channel • Signalling: Use a devoted wavelength counter-propagating on the protection cable
Shared	<ul style="list-style-type: none"> • Switches in the SU_i • One switch in the TN and one switch in the RN • An interconnect fibre failure causes protection switching of every SU_i • The APS protocol communicates between TN, RN and every SU_i • There is only one alarm and one restoring action • Spatial reuse is available for low priority traffic in the protection fibres • Signalling: Use a devoted wavelength counter-propagating on the protection cable 	<ul style="list-style-type: none"> • Switches in the SU_i • N switches in the TN and N switches in the RN • An interconnect fibre failure causes protection switching only in SU_i • Complex APS protocol <ul style="list-style-type: none"> – it only communicates between the TN, RN and every SU_i – there is up to N alarms: one for each SU_i • Spatial reuse is available for low priority traffic in the protection fibres • Signalling: Use a devoted wavelength counter-propagating on the protection cable

Table 1 The main features of the four categories of protection in the direct unidirectional sensor array.

5.1 Dedicated Line Protection

When the working cable is severed between SU_i and SU_{i+1} , there is complete LoS at the RN and so all channels must be carried by the protection cable. The first action is to switch the receiver to attempt to detect P_{out} but only $\lambda_1, \dots, \lambda_i$ will be present. A signal is then sent to the TN to switch all lasers to P_{in} . Thereafter, all channels use the protection infrastructure exclusively and the network management computer sends a request to the network operator's staff to perform a cable repair. The signalling can take place within the existing infrastructure, even when there is a cable failure, by launching the special wavelength λ_s contra-directionally from the RN to the TN within one of the fibres in the protection cable. Furthermore, provided that the protection cable remains intact, it is possible to ensure complete recovery of service even when there are multiple point failures along the working cable.

When one of the working interconnect fibres is broken, the RN detects a LoS on the corresponding channel, which should normally arrive via the working aggregation fibre. However, as all channels are switched collectively at the TN and RN, regaining service from a

single fault requires all N channels to be launched at P_{in} , even though $N - 1$ of them could continue to operate satisfactorily using the working infrastructure. The sequence of switching and signalling at the TN and RN is the same as when the working cable fails. In dedicated line protection operation can be re-established even when several working interconnect fibres have failed. However, one or more channels will be lost completely if some failures are to the working interconnect fibres and the others are to the protection interconnect fibres.

5.2 Dedicated Path Protection

A failure in the working cable between SU_i and SU_{i+1} prevents any channel from reaching the RN via W_{out} . Consequently, N alarms are generated, causing all N switches at the RN to be activated to recover service via the protection aggregation fibre. However, as the branching points are passive 1x2 couplers, the outputs from the sensor units attempt to propagate to the RN via both the working and protection aggregation fibres, irrespective of which distribution fibre conveyed the light from the N lasers in the TN. Consequently, not all switches at the TN must change their state in response to a point failure in the working cable. Channels $i+1, \dots, N$ must be launched by P_{in} , while the others can continue via W_{in} . Signalling is by the same means as in dedicated line protection but the traffic volume is higher because of the need to specify which switches in the TN must change state. Where there are several failures in the working cable, full service recovery can be ensured by activating all switches at the RN but only those switches at the TN corresponding to the isolated sensor units.

Upon failure of the working interconnect fibre to SU_i , the RN detects no power on the corresponding channel. Only λ_i need be switched to the protection infrastructure at the RN and TN and the signalling instruction is very simple. Full service continuity is possible despite multiple failures to interconnect fibres, provided that no more than one interconnect fibre per sensor is affected. As dedicated protection operates on a channel-by-channel basis, they can be to either the working or the protection interconnect fibres. In all cases signalling at λ_s is contra-directional, using one of the fibres in the protection cable.

5.3 Shared Line Protection

When the working cable is cut between SU_i and SU_{i+1} , no channel arrives at the RN and service is regained by requiring all channels to move entirely to the protection infrastructure. Upon detecting the LoS, a telemetry signal at wavelength λ_s is sent from the RN to the TN via the protection distribution fibre. Two separate commands (again at λ_s) are then issued to the switches in all sensor units, requesting a change of state. The TN must signal to SU_1, \dots, SU_i , launching via W_{in} and the RN must signal to SU_{i+1}, \dots, SU_N , launching contra-directionally via W_{out} . Finally, the TN and RN activate their switches so that the N sensor channels are launched and received at P_{in} and P_{out} , respectively. Where spatial re-use is employed, all of the low priority traffic is lost in the event of a failure. Shared line protection cannot tolerate failures in both the working and protection cables. However, it is possible to survive multiple failures to the working cable but signalling to the switches is demanding and it may require external means, such as a radio link.

If one interconnect fibre is cut, every channel must be switched from the working cable to the protection cable. No sensor is unaffected because every BP switch must change state and there is a momentary loss of service while this occurs. If there is spatial re-use, all of the low-priority traffic on the protection cable is completely displaced, even though only one interconnect fibre is cut. It is possible to survive failures to several of the working interconnect fibres or several of the protection interconnect fibres but not combinations of both.

Signalling is more problematical when a working interconnect fibre fails because the 1x2 switch in SU_i is in a state that allows light to enter only by the failed fibre. There are several solutions. The first, as discussed in Section 3, is to provide a radio or other external link but it violates our second requirement for an available architecture. A second option is to change the states of the 1x2 switches in the SU_i periodically and listen for telemetry commands from the RN which state either "all is normal – do nothing" or "there is a failure – activate switching". If the network is used only for sensing services, the option is viable because sensors are seldom interrogated at high frequencies. A third choice is to replace the 1x2 switches in the SU_i by 2x2 cross-bar switches. In normal operation the switches are in the

bar state so that the working interconnect fibres are connected to the sensors, while the protection interconnect fibres are connected to switch controllers. When a fault is detected through a LoS at the RN, a telemetry signal is sent via the protection distribution fibre to all of the switch controllers to instruct them to change their switches to the cross state. Thereafter, the sensors are all connected to their protection interconnect fibres. A fourth possibility is illustrated in Fig. 4, which shows additional fibre connections to permit signalling via one of the distribution fibres by launching from the RN. The commands activate switch controllers located at each SU_i . Unfortunately, all four solutions require intelligence and additional hardware within the SU_i and therefore increase the cost.

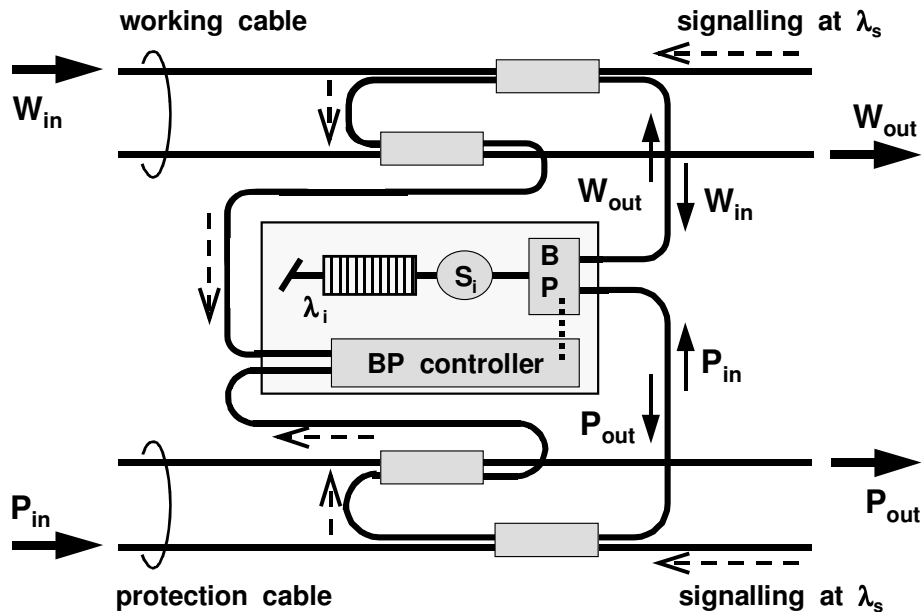


Figure 4 One segment of a direct unidirectional sensor array for use in shared protection. Alternative fibre configuration at the sensor unit SU_i to enable signalling in the event of a failed interconnect fibre without the need for external resources, such as a radio link.

5.4 Shared Path Protection

One failure to the working cable causes total loss of optical power at the RN. N alarms are generated, one for each wavelength, and they require $3N$ actions because all switches throughout the network must be activated to resume service: N at the TN, N at the RN and N at the SU_i . Clearly, the control software is relatively complicated. Upon completion of the switching actions, all traffic is carried by the protection infrastructure, which means that there is complete network failure in the event of cuts to both the working and protection cables in any positions. Nevertheless, it is possible to survive multiple failures to the working cable. In the event of spatial re-use, all low priority traffic on the protection cable is lost if the working cable is damaged in one or more places.

If one interconnect fibre is severed, the signalling between the TN, RN and SU_i and subsequent switching affects only one sensor. This means that $N - 1$ channels propagate entirely by the working cable and only one by the protection cable. The momentary disruption to traffic during post-damage signalling and switching is limited to the affected sensor. Where there is spatial re-use on all N channels, only one of them need displace its low-priority traffic. Due to the channel-by-channel protection, it is possible to survive several failed interconnect fibres. They can be in any combination – working or protection – provided that no more than one interconnect fibre per sensor is affected.

The differences in the signalling requirements between shared path and shared line protection lie in the requests that are made to the switches. All switches are activated in shared line protection but only a sub-set in shared path protection. The physical paths taken by the signalling traffic are the same in both cases. When the working cable is cut all switches in the network must be activated so that operation is entirely by the protection

infrastructure. Therefore, the signalling procedures are as described in Section 5.3. In shared path operation when one of the working interconnect fibres fails, only the three associated switches need be activated. Nevertheless, the same signalling constraints and choices apply as outlined in Section 5.3. Combined failures to working and protection interconnect fibres are more demanding for the signalling and the best means may be as illustrated in Fig. 4 or by an external radio link.

	Dedicated Line	Dedicated Path	Shared Line	Shared Path
Direct Unidirectional Sensor Array	Multiple point failures on the working cable Multiple failures to the working <u>or</u> the protection interconnect fibres Signalling is straightforward	Multiple point failures on the working cable Multiple failures to the interconnect fibres: various locations Signalling is straightforward	Multiple point failures on the working cable Multiple failures to the working <u>or</u> the protection interconnect fibres Signalling is demanding when inter-connect fibres fail	Multiple point failures on the working cable Multiple failures to the interconnect fibres: various locations Signalling is demanding when inter-connect fibres fail
Reversed Unidirectional Sensor Array	Same as direct unidirectional sensor array	N/A	Same as direct unidirectional sensor array	Same as direct unidirectional sensor array
Crossed Unidirectional Sensor Array	Multiple point failures on cable A Multiple failures to the working <u>or</u> the protection interconnect fibres	Multiple point failures on cable A Multiple failures to the interconnect fibres: various locations	N/A	One failure on cable A Multiple failures to the interconnect fibres: various locations
Bidirectional Sensor Array	N/A	Up to one point failure on the distribution cable <u>plus</u> one point failure on the aggregation cable Multiple failures of the interconnect fibres: various locations	N/A	One point failure on the distribution <u>or</u> the aggregation cable Multiple failures of the interconnect fibres: various locations

Table 2 Summary of the topologies and protection categories explored and the number of failures that they can survive. N/A = not available, according to the three criteria stated in Section 1.

6. Alternative Network Topologies

We now propose bus designs with different cabling configurations from the direct unidirectional sensor array. We continue to refer to the four protection categories described

in Section 2 and require the three criteria of network availability stated in Section 1. When one or more criteria cannot be satisfied, we designate the protection category “not available” (N/A). We note that networks which ensure nominally equal transmission impairments between the working and protection infrastructures satisfy a more stringent requirement than self-healing rings for telecommunications [1 – 3]. Furthermore, it is sometimes possible to exceed our criterion of being able to survive one fibre failure at any point and topologies that do so are desirable. The key characteristics of the network designs are summarised in Table 2.

6.1 Reversed Unidirectional Sensor Array

The network topology is illustrated in Fig. 5. It includes a working cable and a protection cable, each containing a distribution and an aggregation fibre and the working and protection cables are each joined to every SU_i by one interconnect fibre. However, Fig. 5 differs from Fig. 2 in the direction of the protection traffic. It travels contra-directionally with respect to the working traffic but the light within each cable travels in one direction, justifying the description “unidirectional”. When the two ends of the network are distinct units, the working lasers are co-located with the protection detectors and vice-versa. For this reason, we refer to them as the “A –” and “B –” ends. However, as discussed in Section 4, the entire network can be folded, as shown in Fig. 3, to co-locate the A – and B – ends. If it is economically viable, the configuration then offers the benefit of simplified signalling.

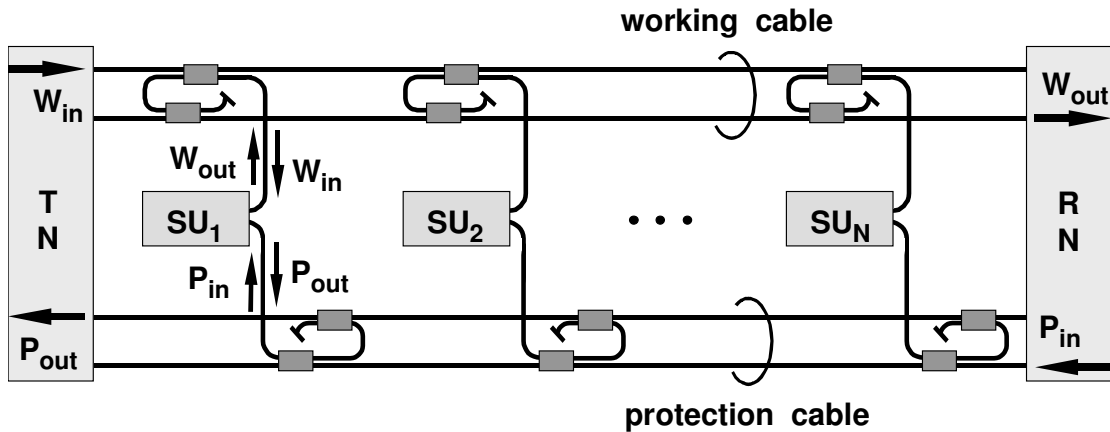


Figure 5 Reversed unidirectional sensor array bus network. SU_i = sensor unit i . W_{in} and W_{out} = working cable: input and output, respectively. P_{in} and P_{out} = protection cable: input and output, respectively. TN = transmitter node, RN = receiver node. The elements within the sensor units are as illustrated in Fig. 2.

One can follow the arguments presented in Section 5 for various failure locations with respect to the four protection categories. All four categories can withstand a single failure in the network at any location and signalling is possible without the need for additional physical infrastructure. Dedicated line, shared line and shared path operation can tolerate the same numbers and combinations of failures as their counterparts in the direct unidirectional sensor array.

Unfortunately, after protection switching dedicated path protection does not satisfy our requirements for transmission impairments. During normal operation, all channels traverse the same numbers of couplers and fibre spans but this is no longer so after protection switching. As a concrete example, consider a failure in the working cable between SU_1 and SU_2 in Fig. 5. After protection switching has occurred, sensor 1 is served by launching by W_{in} and receiving by P_{out} . In contrast, the other channels must be launched by P_{in} and therefore encounter greater losses on the way to their receivers. One solution could be to program all switches in the A- and B- ends to act collectively when the working fibre fails, so that the network behaves as if it has dedicated line protection. In that case, switching of individual fibres is used only in response to failed working interconnect fibres. However, the benefit of providing the $2N$ switches is then relatively small and so we regard dedicated path protection as N/A, as marked in Table 2.

Telemetry signalling is most straightforward in dedicated line protection. When the working cable fails, all channels at W_{out} are lost. The B-end then uses λ_s in one of the protection fibres to instruct all receivers in the A-end to switch to P_{out} and lastly the B-end launches all channels via P_{in} . When the working interconnect fibre to SU_i fails, the B-end launches all channels via P_{in} and signals the A-end to accept all channels via P_{out} .

Signalling is more complicated in shared line and shared path protection. In the event of working cable failure, the procedure is the same as in the direct unidirectional sensor array, in which signals are launched from both ends on the working infrastructure to instruct the 1x2 switches to change their state. Furthermore, the same difficulties apply in the event of a failed working interconnect fibre and the solutions that can be adopted are as explained in Section 5.3.

6.2 Crossed Unidirectional Sensor Array

One segment of a crossed unidirectional sensor array is shown in Fig. 6. The working distribution fibre shares a cable, designated "cable A", with the protection aggregation fibre. Similarly, the working aggregation and protection distribution fibres share "cable B". The working and protection lasers are in the TN, while the working and protection receivers are in the RN.

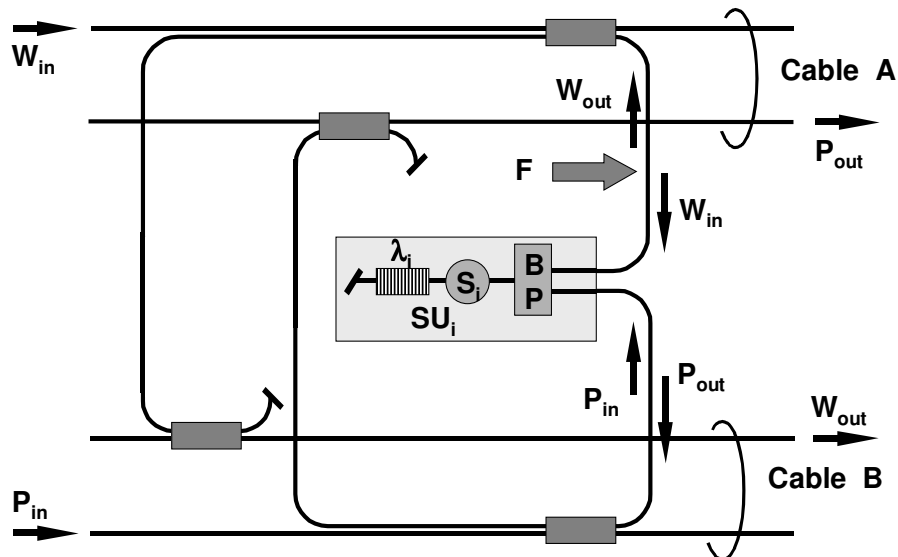


Figure 6 One segment of the crossed unidirectional sensor array. BP = branching point, SU_i = sensor unit i , S_i = sensor element i . W_{in} and W_{out} = working cable: input and output, respectively. P_{in} and P_{out} = protection cable: input and output, respectively. F = point where a failure is most problematical.

There is a complicated arrangement of interconnect fibres joining the sensor units with cables A and B, which could increase the installation costs. Moreover, careful layout of the cabling for the interconnect fibres is required to ensure that their relative complexity does not lead to greater failure probabilities. When an interconnect fibre does fail, it has the most serious consequences at the position marked F on Fig. 6. A failure at F prevents light from entering or leaving the sensor unit, which means that the working infrastructure cannot be used for signalling to the sensor units in those protection categories that require it. In analysing the network, we have always considered such failures, as they are the worst case.

There are two grounds upon which the crossed unidirectional sensor array topology can be justified. The first is that the two transmitter sets (W_{in} and P_{in}) are co-located and the two receiver sets (W_{out} and P_{out}) are co-located. Consequently, in contrast to the reversed unidirectional sensor array, there is less incentive to configure the whole network as a physical ring, with its potentially higher costs of civil works. The second possible justification is tolerance to certain combinations of failures.

Consideration of the unidirectional sensor array reveals that shared line protection cannot recover service from all sensors when either cable A or cable B is cut and it is therefore designated N/A. Depending on the position of the cable damage, some input channels cannot arrive at their target sensors, while others do not have a path to their receivers. However, the other three protection categories enable continuity of service after single point failures. Furthermore, as Table 2 summarises, dedicated line and dedicated path protection can withstand multiple failures to either cable A or cable B but none of the protection categories is resilient to combinations of failures to cables A and B. When there is one failure on each cable all three of the available categories can regain service of the sensors that lie between the two points of failure but no other.

All three of the available protection categories can survive multiple failures to the working interconnect fibres or the protection interconnect fibres. Additionally, thanks to their channel-by-channel connectivity, the two categories of path protection can survive a wider combination of failures to the interconnect fibres: some to the working and others to the protection infrastructure, provided that at least one per sensor remains functional.

Signalling by the use of one of the fibres in cable B is possible in dedicated line and dedicated path protection. This applies whether the failure is at one or more locations on cable A or to several of the interconnect fibres. Signalling is more technically demanding for shared path protection when an interconnect fibre is cut at position F because the sensor unit's switch is connected to the failed fibre. (The same applied in the direct and reversed unidirectional sensor arrays.) Therefore, one of the solutions discussed in Section 5.3 will have to be adopted, with adverse implications for costs.

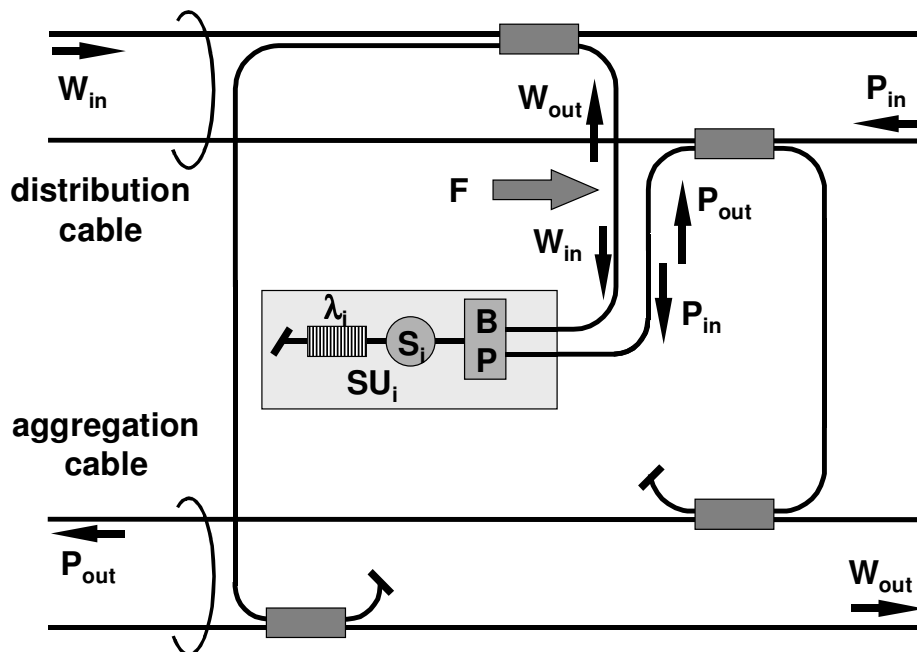


Figure 7 One segment of the bi-directional sensor array. BP = branching point, SU_i = sensor unit i , S_i = sensor element i , W_{in} and W_{out} = working cable: Input and output, respectively. P_{in} and P_{out} = protection cable: input and output, respectively. F = point where a failure is most problematical.

6.3 Bi-directional Sensor Array

One segment of the bi-directional sensor array is shown in Fig. 7. There are two cables that perform the backbone function, transporting all wavelengths and they are termed the “distribution” and the “aggregation” cables. The word “bi-directional” refers to propagation in these cables and not in the individual fibres. As Fig. 7 shows, the interconnect fibres are in a slightly more complicated configuration than the direct and reversed unidirectional sensor

arrays but, as we argue here, it can confer the benefit of increased survivability in some circumstances.

Dedicated and shared line protection are not available in the bi-directional sensor array. In line protection the APS protocol requests the collective switching in one common action. However, if the distribution cable should be broken, there is no single action that enables all of the sensors to receive the launched signals and this applies irrespective of whether the SU_{*i*} contain 1x2 couplers or switches.

In dedicated path protection each channel is individually launched on to either the working or the protection distribution fibre, but not both. Upon reaching its target sensor, it attempts to propagate via both the working and protection infrastructures. When there is one failure on the distribution cable between SU_{*i*} and SU_{*i+1*}, channels 1, ... , *i* are launched and received by W_{*in*} and W_{*out*}, respectively and channels *i* + 1, ... , N are launched and received by P_{*in*} and P_{*out*}, respectively. In this way, all three conditions of acceptable operation can be satisfied. In particular, all channels traverse the same number of couplers and fibre spans.

Dedicated path protection offers the desirable feature of being able to survive one failure in each of the distribution and aggregation cables. Figure 8 shows failure pairs, F_{*x*} – F_{*x*}, F_{*y*} – F_{*y*} and F_{*z*} – F_{*z*}. By careful selection of the launch points (W_{*in*} or P_{*in*}) and receiver points (W_{*out*} or P_{*out*}) on a channel-by-channel basis, it is possible to regain service after all such combinations of failures. However, there are three important limitations. Firstly, service continuity cannot be provided when there are multiple failures in either the distribution or aggregation cables. Secondly, double failures of the types shown in Fig. 8 block all possibility of signalling within the network's own fibre infrastructure and so alternative means, such as a radio link are unavoidable. Thirdly, surviving combined failures requires a selection of channel launch and reception points that violate our requirement that all channels experience nominally equal transmission impairments.

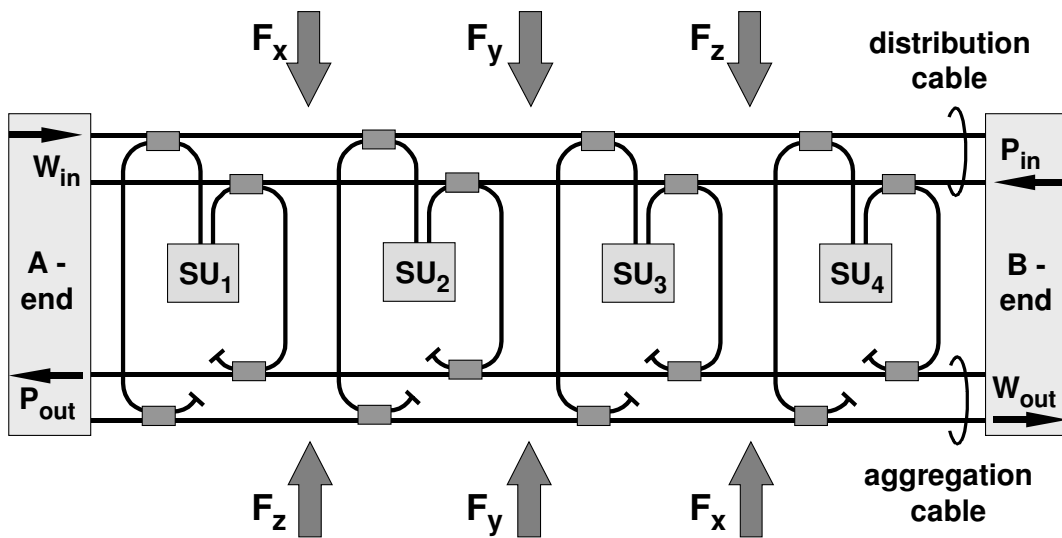


Figure 8 Bi-directional sensor array with four sensors illustrating combinations of failure positions from which service can be regained when using dedicated path protection.

A failure in the working interconnect fibre is most problematical at position F on Fig. 7 because it prevents the sensor from receiving any input from the working infrastructure. Signalling must then be by the protection infrastructure. Nevertheless, even when they are at the F-positions, dedicated path protection is resilient to multiple failures in the interconnect fibres. Owing to the channel-by-channel connectivity of path protection, some failures can be to the working interconnect fibres and others to the protection interconnect fibres, provided that at least one per sensor remains intact.

In shared path protection each sensor is protected individually. Once one or more channels experiences a LoS, switching takes place at the TN, the appropriate SU_i and the RN and the affected channels use the protection infrastructure entirely. As there is never an interchange of any channel between the working and protection infrastructures, full service can be regained if there is at most one failure to the distribution cable or one failure to the aggregation cable. Channels are lost in the event of multiple or combined failures. However, owing to the channel-by-channel protection, it is possible to survive failures in various combinations of the interconnect fibres: some to the working interconnect fibres and others to the protection interconnect fibres. The condition is that, for any one SU_i , at least one of its interconnect fibres remains functional.

7. Conclusion

We have proposed and critically compared novel topologies for sensor networks that use protection switching to survive damage to the fibre infrastructure at one or more points. Each design is a ladder bus in which the sensors are uniquely identified by wavelength using fibre Bragg gratings. We have considered four protection categories – dedicated line, dedicated path, shared line and shared path – which have direct counterparts in telecommunications networks. Telemetry signalling, which is the means to communicate the presence of a failure and request that the appropriate action be taken to recover service, is an integral aspect of protection switching. The physical topology, the protection category and the means for signalling must be considered together when evaluating a network design.

We have identified three criteria for an architecture to be viable (“available” in our terminology): It must (1) withstand at least one fibre failure, which can be at any location, (2) perform the necessary signalling within the existing fibre infrastructure and (3) be configured so that in traversing the network all channels experience nominally equal transmission impairments in both their working and protection states. Collectively, these criteria are demanding but there are several combinations of topologies and protection categories that can satisfy them, as summarised in Table 2. Where relevant, we have indicated potentially expensive options but we have not used cost as an availability criterion. What matters is holistic costs, which cannot be quantified without knowing the sensing application, the network’s physical dimensions and whether other services, such as data communications, are also carried.

The choice between dedicated and shared protection is important because, once the network is installed, it is disruptive to upgrade from one to the other by replacing all of the BPs, APS software and signalling equipment. The critical factors that determine the decision are the cost, the complexity of the APS software, the ease of signalling, the ability to withstand multiple failures, the optical transmission impairments and the need for spatial reuse. We believe that in all topologies dedicated protection offers clear advantages from the point of view of cost, simplicity of APS software and ease of signalling. Moreover, dedicated path protection can withstand multiple failures in some topologies. Where shared protection is used, it must be justified by its lower losses at the BPs and its ability to offer spatial reuse in those circumstances that warrant it. However, unless there is a strong need for these two attributes, dedicated protection is preferable in our view.

Whether line or path protection is selected depends on costs, complexity of APS software and the ability to withstand multiple failures. The signalling connectivity requirements are the same in both cases and, although the signalling traffic volume is greater in path protection, it is unlikely to be a deciding factor. Where the topology permits it, we believe that a viable strategy is to install dedicated line protection at the network’s inception and to upgrade to dedicated path protection, should the need for greater resilience subsequently arise. Upgrading requires the installation of N switches and more advanced APS software in each end node. In this way, the capital expenditure is spread over time. One compromise strategy could be to identify sensors that are especially critical or vulnerable and protect them individually with their own switches at the end nodes, while the other channels are protected collectively with common switches. A hybrid path/line strategy is therefore possible.

Correctly selecting the network topology is crucial as it determines the layout of the cabling, the revision of which might never be affordable. We believe that the direct unidirectional sensor array is the most versatile choice. It offers all four protection categories, a simple configuration of interconnect fibres and the ability to withstand multiple failures to the working cable or to the working interconnect fibres. Furthermore, dedicated path and shared path protection offer resilience to combined failures of the working and protection interconnect fibres, provided that at least one per sensor remains intact.

We have studied other network topologies but none offers the consistent performance of the direct unidirectional sensor array. Sometimes the interconnect fibres are folded in a manner that causes slight concern for their construction costs and reliability. Alternatively, line and path protection might not both be available and so upgrading is not possible. However, we draw attention to the bi-directional array with dedicated path protection. In addition to satisfying all three of our availability criteria, it can survive multiple failures in the interconnect fibres (working or protection), subject to the limitation of one per sensor. Moreover, if the requirements for no external signalling and nominally equal transmission impairments can be relaxed, the bi-directional sensor array with dedicated path protection can recover service after one failure in each of the distribution and aggregation cables. The value of the tolerance to such double failures depends on the sensing application of the network and the various geographical factors that determine the cable damage statistics.

In conclusion, we have presented novel designs of optical fibre bus networks for application to the multiplexing of arrays of sensors which can withstand one or more point failures. We have compared many options for network topology and protection category and we believe that it is possible to identify clear preferences. Although we cannot be prescriptive for all circumstances, a good operational choice will often be the network illustrated in Fig. 2 of this paper, which is called the direct unidirectional sensor array. Where the network is used exclusively for sensing services, we prefer dedicated path protection on grounds of resilience to multiple failures, simplicity of signalling and APS protocols and acceptably low costs. Should cost be an initial constraint, it is possible to install dedicated line protection and upgrade to path protection when circumstances permit.

Acknowledgement

Financial support for this work was provided by the Spanish Ministerio de Educación y Ciencia, project number TEC2004-05936-C02-01/MIC.

References

- [1] T. H. Wu, "*Fibre Network Service Survivability*", Artech House, (1992).
- [2] R. Ramaswami and K.N. Sivarajan, "*Optical Networks: A Practical Perspective*", second edition, Morgan Kaufmann, (2002).
- [3] T. E. Stern and K. Bala, "*Multiwavelength Optical Networks: A Layered Approach*", Addison Wesley Longman Inc., (1999).
- [4] A. A. M. Saleh and J. N. Simmons, "*Architectural Principles of Optical Regional and Metropolitan Access Networks*", *Journal of Lightwave Technology*, **17** (12), 2431-2448, (1999).
- [5] K. Hotate, "*Fiber Sensor Technology Today*", *Japanese Journal of Applied Physics*, **45**, (8B), 6616–6625, (2006).
- [6] P. C. Peng, H. Y. Tseng and S. Chi, "*Self-healing Fibre Grating Sensor System using Tunable Multiport Fibre Laser Scheme for Intensity Division Multiplexing*", *Electronics Letters*, **38** (24), 1510-1512, (2002).
- [7] P.C. Peng, S. Chi, "*A Reliable Architecture for FBG Sensor Systems*", *Microwave and Optical Technology Letters*, **39** (6), 479-482, (2003).

- [8] K.T.V. Grattan, B.T. Meggitt (editors), "*Optical Fiber Sensor Technology*", Volumes 1 – 4, Kluwer Academic Publishers, (1998 -2000).
- [9] A. Dandridge and C. Kirkendall, "*Passive Fiber Optic Sensor Networks*", Chapter 21 of "*Handbook of Optical Fiber Sensing Technology*", J.M. Lopez Higuera, (Editor), Wiley, (2002).
- [10] J. M. Senior, S. E. Moss, S. D. Cusworth, "*Multiplexing Techniques for Non-interferometric Optical Point-Sensor Networks: A Review*", *Fiber and Integrated Optics*, **17**, 3-20, (1998).
- [11] V. Montoya, M. López-Amo and S. Abad, "*Improved Double-Fiber-Bus with Distributed Optical Amplification for Wavelength Division Multiplexing of Photonic Sensor*", *IEEE Photonics Technology Letters*, **12** (9), 1270-1272, (2000).
- [12] R. Hernandez Lorenzo, M. López-Amo, P. Urquhart, "*Single and Double Distributed Optical Amplifier Fiber Bus Networks with Wavelength Division Multiplexing for Photonic Sensors*", *IEEE Journal of Lightwave Technology*, **16** (4), 485 – 489, (1998).
- [13] M.-J. Li, M.J. Soulliere, D.J. Tebben, L. Nederlof, M.D. Vaughn, R.E. Wagner, "*Transparent Optical Protection Ring Architectures and Applications*", *IEEE Journal of Lightwave Technology*, **23** (10), 3388-3403, (2005).
- [14] G. P. Agrawal, "*Nonlinear Fiber Optics*", 3rd Edition, Academic Press, (2001), see especially Chapter 9.
- [15] N.J. Frigo, P.P. Iannone, K.C. Reichmann, X. Zhou, M.W. Stodden, "*Centralized In-Service OTDR Testing in a CWDM Business Access Network*", *IEEE Journal of Lightwave Technology*, **22** (11), 2641-2652, (2004).
- [16] C.W. Hodgson, J.L. Wagener, M.J.F. Digonnet, H.J. Shaw, "*Optimization of Large-Scale Fiber Sensor Arrays Incorporating Multiple Optical Amplifiers – Part I: Signal to Noise Ratio*", *IEEE Journal of Lightwave Technology*, **16** (2), 218-223, (1998).
- [17] C.W. Hodgson, D.A. Frederick, "*Architecture for Large Optical Fiber Array Using Standard 1x2 Couplers*", US Patent 6,768,829 B2, (2004).
- [18] S. Abad, M. López-Amo, I.R. Matias, "*Active Fiber Optic Sensor Networks*", Chapter 22 of "*Handbook of Optical Fiber Sensing Technology*", J.M. Lopez Higuera, (Editor), Wiley, (2002).
- [19] S. Díaz, G. Lasheras, M. López-Amo, P. Urquhart, C. Jáuregui, J.M. López-Higuera, "*Wavelength-Division-Multiplexing Distributed Fiber Raman Amplifier Bus Network for Sensors*", *Proceedings of the 17th Optical Fiber Sensors Conference*, SPIE Proceedings **5855**, 242-245, (2005).
- [20] P. Aneli, M. Soto, "*Evaluation of the APS Protocol for SDH Rings Reconfiguration*", *IEEE Transaction on Communications*, **47** (9), 1386-1393, (1999).
- [21] R.A. Perez-Herrera, S. Díaz, P. Urquhart, M. López-Amo, "*A Resilient Raman-Amplified Double Ring Network for Multiplexing Fiber Bragg Grating Sensors*", *Proceedings of the SPIE* **6619**, 66193E-1 – 66193E-4, 3rd European Workshop on Optical Fibre Sensors, Naples Italy, (4 – 6 July 2007).
- [22] H. Ji, K. Park, H. Chung, E. Son, K. Han, S. Jun, Y. Chung, "*Optical Performance Monitoring Techniques Based on Pilot Tones for WDM Network Applications*", *Journal of Optical Networks*, **3**, 510-533, (2004).