Optical Fiber Bus Protection Network to Multiplex Sensors: Experimental Validation of Self-Diagnosis

Rosa Ana Perez-Herrera, Paul Urquhart, Marcel Schlüter, Silvia Diaz, and Manuel Lopez-Amo

***Abstract*—The experimental demonstration of a resilient wavelength division multiplexed (WDM) fiber bus network to interconnect sensors is reported. The network recovers operation after failures and it performs "self-diagnosis", the identification of the failed constituent(s) from the patterns of surviving end-to-end connections at its operating wavelengths. We provide clear evidence for the channel arrivals predicted by theory. In doing so, we explore the potential for spurious signals caused by reflections from broken fiber ends. Appropriate precautionary measures, especially the imposition of electronic thresholds at the receivers, can greatly reduce the scope for false diagnoses. Software to predict the failure site within the network from the arriving channels at the receivers is also reported. We describe how to coordinate self-diagnosis with protection switching so as to reduce the momentary service interruption.**

***Index Terms*—**Network fault tolerance, Optical fiber LAN, Protection, Sensors

I. INTRODUCTION

OPTICAL fiber offers many advantages for the networking of sensors [1], [2], especially when accidental sparking in combustible media, signal interruptions during bad weather, line-of-sight blockage by natural and man-made structures, and external electromagnetic interference are concerns. However, in common with telecommunications [3], [4], a network's fiber and components can be damaged by human activities or natural events, rendering some or all of its sensors inoperative. Service loss after failures is most detrimental in safety and security applications. Resilient architectures, which recover operations by redirecting signals over duplicated infrastructure, are thus of growing interest [5], [6].

Re-establishing full service is not the only operating challenge; failure sites must be located quickly and cheaply in preparation for repairs. Upon suffering damage, a network is in an unprotected state and might not survive a second destructive event. Although optical time domain reflectometry (OTDR) [7] is helpful, its traces are difficult to interpret in multi-branched topologies. Automated identification of the failed constituents is, therefore, very desirable [8]. It reduces costs and the mean time to repair.

A novel means of specifying failure sites within a WDM resilient fiber bus network, called "self-diagnosis", has been proposed and mathematically modeled [9]. In this paper we report an experimental study of its viability by providing evidence in favor of the model. In particular, we explore the influence of end reflections after fibers have been broken, possibly causing multi-path signal transits through the network. Our results indicate that reflections do *not* prevent the functioning of self-diagnosis. We also describe simple software for the unique identification of the failed elements resulting from any single destructive event and we explain how to coordinate self-diagnosis with service recovery.

II. SELF-DIAGNOSIS: OPERATING PRINCIPLES

The network is shown in Fig. 1 (top). Detailed descriptions are presented in Refs. [9] to [11], but here we concentrate on how it enables self-diagnosis. It is a symmetrical bus structure, in general with $(N + 1)$ blocks to interconnect a transmitter node (TN), on the left, via an array of N sensors to a receiver node (RN), on the right. (In the diagram $N = 3$ to depict our experiment.) Its "working" and "protection" infrastructures are demarcated by a horizontal axis. Block 0 is merely two pairs of connecting fibers. The other N blocks have two pairs of fibers to traverse the network, symmetrical interconnecting fibers, four broadband couplers, and a sensor unit (SU-i; $i = 1, 2, \ldots, N$). All elements have unique names and the terminology for Block i is marked in Fig. 1 (bottom). Each SU is a 1×2 passive splitter, a fiber Bragg grating (FBG) and a sensor. The grating in SU-i reflects only λ_i, the block's "characteristic wavelength", to provide unique sensor identification.

The sensors can be of many electrically passive types to impose an intensity, polarization, or phase modulation. Where a lower channel spectral density can be tolerated, the FBGs themselves can act as wavelength-modulated sensors [12].

In normal operation unmodulated light at the N sensing wavelengths is launched at *either* point T_1 *or* point T_4 in the TN. The couplers direct all wavelengths to every SU but each

Manuscript received February xx, 2012. This work was funded by the Spanish Ministry of Education and Science, project TEC2010-20224-C02-01.

R.A. Perez-Herrera, P. Urquhart, S. Diaz, and M. López-Amo are with the Universidad Pública de Navarra, Department of Electronic and Electrical Engineering, Campus de Arrosadía, 31006 Pamplona, Spain. (e-mail: Paul.Urquhart@unavarra.es)

M. Schlüter was with Hochschule Niederrhein, Department of Electrical Engineering and Computer Science, Reinarzstraße 49, 47805 Krefeld, Germany. He is now with Bertrandt Ingenieurbüro GmbH Oskar-Schindler-Str. 10, 50769 Köln, Germany (e-mail: eagle-ms@gmx.net).

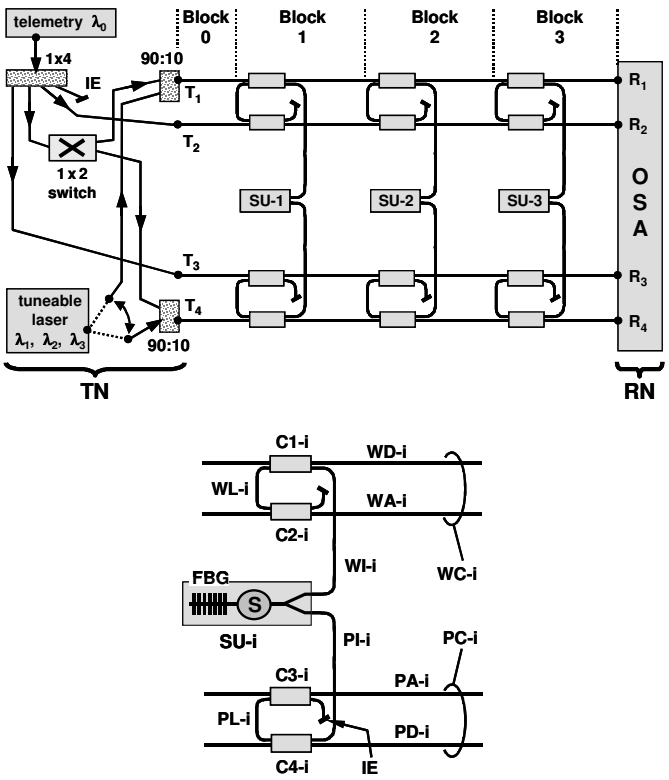

Fig. 1. Resilient bus network for the multiplexing of sensors, housed in sensor units (SU). Top: experimental assembly. Bottom: structure and terminology used for Block i, (i = 1, 2, …, N). T_k and R_k are the transmitter and receiver points, respectively, where k = 1, 2, 3, 4. They are within the transmitter node (TN) and receiver node (RN). The elements are designated "W" and "P" for working and protection infrastructures, respectively. C1 to C4: the four couplers within the block. The fibers designations are: "A" (aggregation), "D" (distribution), "I" (interconnect) and "L" (coupler-to-coupler link). "C" is the cable, consisting of "A" and "D" fibers. IE: refractive index matched fibre end. OSA = optical spectrum analyzer.

FBG reflects only its characteristic wavelength. Thus, one modulated channel exits each SU and progresses to the RN via the following blocks. All channels arrive at the RN at points R_2 *and* R_3. A switch directs light from *either* R_2 *or* R_3 to a demultiplexer and receivers. Light launched at T_1 also bypasses the SUs and transmits to the point R_1 (but it cannot reach R_4). Being unmodulated, it plays no role in sensing, but it is required for self-diagnosis. By symmetry, channels sent from T_4 arrive unmodulated at R_4, but never at R_1.

A *single* element failure can be recovered by "dedicated line protection", which uses one switch for all N channels in each of the TN and RN. Activating either one or both switches gives the flexibility to regain full service.

In normal operation all wavelengths have six available end-to-end connections: $T_1 \rightarrow R_1$, $T_1 \rightarrow R_2$, $T_1 \rightarrow R_3$, $T_4 \rightarrow R_2$, $T_4 \rightarrow R_3$, and $T_4 \rightarrow R_4$. However, after a failure occurs, at least one wavelength cannot achieve all six. By using the protection switches, the network can be interrogated at all wavelengths to learn which connections remain intact. The key feature, which enables self-diagnosis, is that the patterns of six connections correlate with the failure site and so provide its identification.

Digital telemetry channels provide signaling between the end nodes; the downstream (TN→RN) and upstream (RN→TN) channels are at wavelengths λ_0 and λ_u, respectively. λ_0 has a key secondary role in self-diagnosis. By suitable choice of its launch points, λ_0 acts as the characteristic wavelength of Block 0, even though there is no FBG. It is launched from (T_1, T_2, & T_3) if λ_1, λ_2, …, λ_N are launched from T_1, but (T_2, T_3, & T_4) if they are launched from T_4. For the purpose of self-diagnosis, λ_0 is treated the same as the N sensing channels. Therefore, there are $(N + 1)$ blocks and $(N + 1)$ downstream wavelengths to interrogate them.

The network is modeled by a binary state connectivity analysis [10]. A "connection coefficient" is assigned to each element; its value is either unity or zero to specify "fully functional" or "failed", respectively. Every channel has binary "powers" of 1 or 0 to designate its presence or absence. Six-element "connectivity vectors", one for each wavelength, specify the overall network status. At an interrogating wavelength λ_j, a failure in Block m ($0 \le m \le N$) has the vector

$$X_{j,m} = [x_{j,m}(T_1 \rightarrow R_1), x_{j,m}(T_1 \rightarrow R_2), x_{j,m}(T_1 \rightarrow R_3), x_{j,m}(T_4 \rightarrow R_2), x_{j,m}(T_4 \rightarrow R_3), x_{j,m}(T_4 \rightarrow R_4)] \quad . \qquad (1)$$

Each element is either 1 or 0. When one component, in Block m, has failed, an N-sensor network is uniquely characterized by three connectivity vectors, written $X_{j<m}$; $X_{j=m}$; $X_{j>m}$. Their subscripts specify the relationship between the indices j and m, both of which lie in the range 0, 1, …, N. The format $X_{j<m}$; $X_{j=m}$; $X_{j>m}$ means that the vectors corresponding to the blocks that precede Block m are all the same ($X_{j<m}$), Block m itself is represented by $X_{j=m}$ and the vectors for the blocks that follow Block m are all the same ($X_{j>m}$).

We provide an example: a network of five sensors, and thus six blocks, suffers a severed working interconnect fiber in Block 3 (WI-3). Scanning the six end-to-end connections for all six launched wavelengths gives: 1,1,1,1,1,1-1,1,1,1,1,1-1,1,1,1,1,1-1,0,0,0,1,1-1,1,1,1,1,1-1,1,1,1,1,1. This is a unique sequence and a single failure site can be identified from it. Its X-vectors are stated as $X_{j<m}$; $X_{j=m}$; $X_{j>m}$ = [1,1,1,1,1,1]; [1,0,0,0,1,1]; [1,1,1,1,1,1], where m = 3. Indeed, there is a yet more concise statement of the end-to-end connections. Each X-vector consists of 1s and 0s and so is the equivalent of a binary number, which can be converted to a decimal in the range 0 – 63. Thus, the single failure WI in Block m is specified by the decimal code $D_{j<m}$; $D_{j=m}$; $D_{j>m}$ = 63; 35; 63. Given we know that N = 5 and m = 3, it is unambiguous.

III. Experiment

Our configuration was the three-sensor network in Fig. 1. The fibers were single mode and every coupler in the network under test was 10% with negligible spectral variations over the operating range. The 10% ratios were not optimal but they easily satisfied our needs. No sensors were present in the SUs so as to concentrate on the network's end-to-end connectivity. All fiber spans were a few meters, but they could be much longer without causing marked degradation. (For example, a resilient amplified network on the scale of a campus with 40

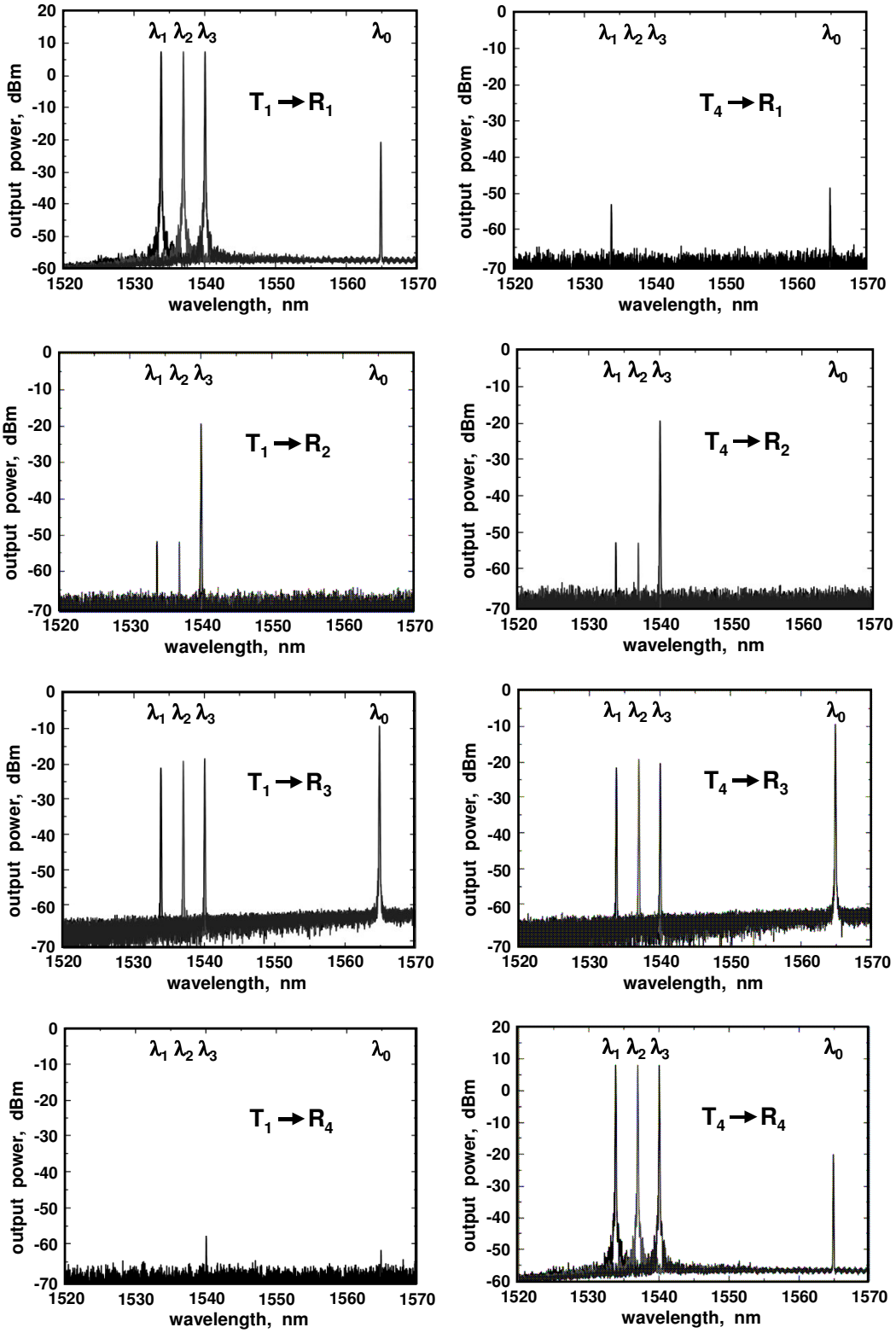

Fig. 2. Received spectra when the working aggregating fiber in Block 2 (WA-2) is severed. The transmission and reception points, T_k and R_k, where k = 1, 2, 3, 4, were as marked on Fig. 1.

sensors and optimized couplers has been modeled [11] and a 46 km unprotected double bus has been experimentally demonstrated [13].) The gratings in SU-1, SU-2 and SU-3 reflected at 1534.0, 1537.3 and 1540.0 nm, respectively. These wavelengths were dictated merely by component availability. (When the FBGs themselves are not wavelength-modulated sensors, costs are lowered by conforming to the ITU-T dense WDM spectral grid [14].)

The sensing wavelengths were launched from a tunable laser at points T_1 or T_4, but never simultaneously. Its emitted

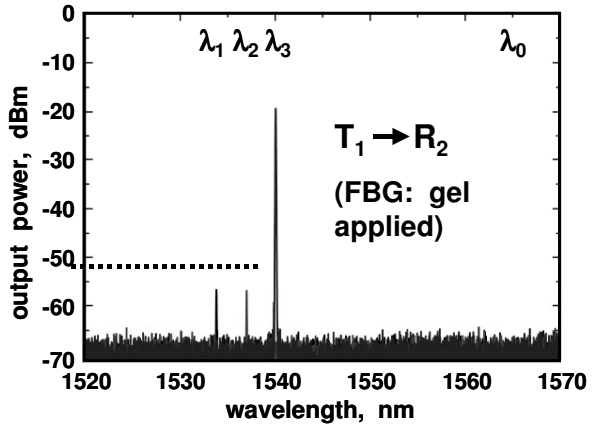

Fig. 3. Received spectrum when the failure is at WA-2. Transmission and reception points: T_1 and R_2, respectively. The reflection from the distal end of the FBG in SU-3 was suppressed. Horizontal dotted line: level of the subsidiary peaks with no reflection suppression.

power was 9.6 dBm and it was tuned to match each FBG in turn. One of the network's advantages is that its end-to-end losses are almost identical for every channel. Thus, the received signal powers at λ_1, λ_2 and λ_3 were always within a narrow range, but slight differences existed owing to (a) the splices to repair the fibers that we deliberately broke and (b) small variations in the gratings' peak reflectances. A separate continuous wave laser at 1565 nm with a power of 1.0 dBm emulated a telemetry channel at λ_0. It was divided three ways by a 1×4 splitter and launched, via a 1×2 switch with a loss of 0.9 dB, into either (T_1, T_2 & T_3) or (T_2, T_3 & T_4), fulfilling the role of a characteristic wavelength for Block 0.

The arriving signals were captured at points R_1, …, R_4 by an optical spectrum analyzer (OSA) with a dynamic range sufficient to detect weak signals from reflections and/or multi-path transits through the network. (Operating networks would often use FBG interrogators, with a sensitivity of around –50 dBm, which is two orders of magnitude worse than the OSA.) We used no signal averaging and so the instantaneous noise floor was always observed. Our aim was to be sure that self-diagnosis can be performed quickly and dependably for fear that a second failure might follow. Moreover, sensing data is lost during the performance of self-diagnosis; see Section V.

The free ends of all couplers C2 and C3 were reflection-suppressed; an operating network would always include this feature. In contrast, if fibers in the field are accidentally severed, their exposed ends reflect ~4% of any incident light. (The value depends on the end angle, the presence of water or dirt, etc.) Thus, our deductions of the surviving channels were made without suppressing reflections from failed fibers.

We have examined the end-to-end connections at the four launched wavelengths for a representative sample of failures caused by single destructive events. All spectra for the six connections in the X-vectors were recorded. We also monitored $T_1 \rightarrow R_4$ and $T_4 \rightarrow R_1$ to ensure an absence of multi-path transits originating from unwanted reflections.

Our first measurements were of a fully intact network to form a control, against which all others were compared. All four wavelengths made the six end-to-end connections and so the corresponding network state was represented by the predicted decimal code $D_{j<m}$; $D_{j=m}$; $D_{j>m}$ = 63; 63; 63. Every received spectral line could be attributed to a launched signal and all signal-to-noise ratios exceeded 40 dB, which is more than sufficient for most sensing applications [1], [2]. The spectra for the $T_1 \rightarrow R_4$ and $T_4 \rightarrow R_1$ connections were broadband noise, with no other discernable features.

TABLE I
THE FAILURE SITES TESTED, MEASURED BINARY CONNECTIONS AT THE FOUR LAUNCHED WAVELENGTHS, AND THE PREDICTED DECIMAL CODES [9].

Failure Site	X_0	X_1	X_2	X_3	Decimal code
no fail	111111	111111	111111	111111	63; 63; 63
PD-0	111110	111000	111000	111000	62; 62; 56
PA-1	110101	110101	111111	111111	53; 53; 63
WA-2	101011	101011	101011	111111	43; 43; 63
WL-2	111111	111111	101011	111111	63; 43; 63
PI-2	111111	111111	110001	111111	63; 49; 63
WC-3	001011	001011	001011	001011	11; 11; 7
PL-3	111111	111111	111111	110101	63; 53; 63
SU-3	111111	111111	111111	100001	63; 33; 63

Fig. 2 shows the eight spectra after we severed WA-2, the working aggregation fiber in Block 2. Our telemetry channel at λ_0 had a longer wavelength than the others and a different launched power [11]. The $T_1 \rightarrow R_1$ and $T_4 \rightarrow R_4$ spectra display the highest signal powers because their wavelengths λ_1, λ_2 and λ_3 bypassed the sensor units. The plots for $T_1 \rightarrow$ (R_1, R_2 & R_3) and $T_4 \rightarrow$ (R_2, R_3 & R_4) reveal that the patterns of the six end-to-end connections are 101011, 101011, 101011 and 111111 for the wavelengths λ_0, λ_1, λ_2 and λ_3, respectively. Therefore, they correspond to the vectors $X_{j<m}$; $X_{j=m}$; $X_{j>m}$ = [1,0,1,0,1,1]; [1,0,1,0,1,1]; [1,1,1,1,1,1], where m = 2, and the decimal code is $D_{j<m}$; $D_{j=m}$; $D_{j>m}$ = 43; 43; 63, as required [9].

The plots in Fig. 2 exhibit subsidiary peaks at wavelengths where the end-to-end connections are expected to be zero. For example, $T_1 \rightarrow R_2$ has features at 1534 nm (λ_1) and 1537.3 nm (λ_2). They are 34 dB below the peak at 1540 nm (λ_3), which is a true connection. Moreover, $T_1 \rightarrow R_4$ and $T_4 \rightarrow R_1$ show lines (at 1534, 1540 and 1565 nm) above the noise but they are much weaker than the peaks in the six other spectra. All such minor peaks are easily distinguishable from the genuine ones. If need be, installed networks could use electronic thresholds to differentiate between real and spurious signals. In our network, an appropriate level would correspond to an optical power in the range –45 to –35 dBm. However, it is important to understand the origins of the low magnitude peaks. They might not matter when there are only three sensors, but larger networks, perhaps with amplifiers [11], can allow more multi-path transits and thus stronger spurious arrivals.

The spectrum in Fig. 3 is the direct equivalent of $T_1 \rightarrow R_2$ in Fig. 2, except that we applied a refractive index matching gel to the distal end of the FBG in SU-3. The fiber termination acted as a weak broadband mirror with a reflectance below the

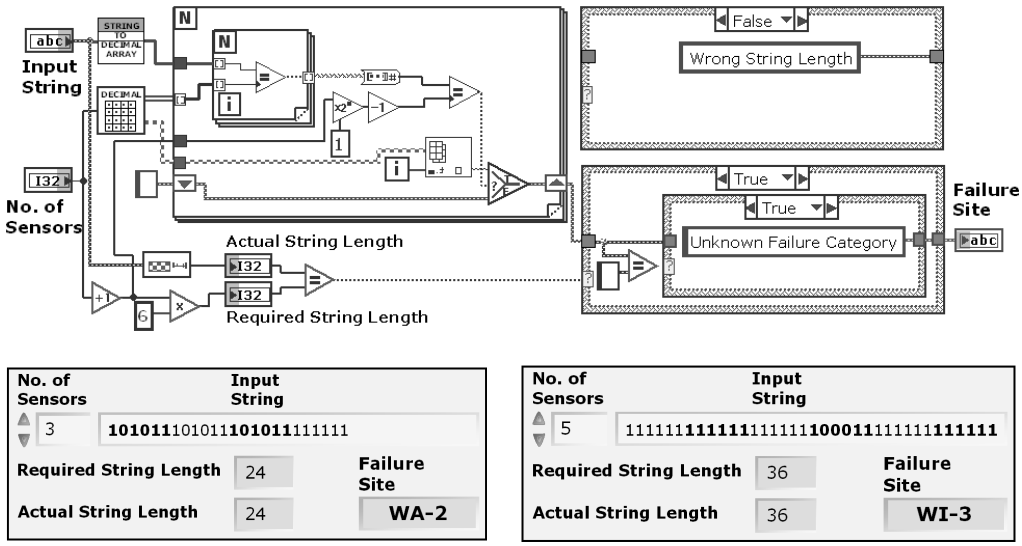

Fig. 4. Top: Block diagram of the main internal connections to form the LabVIEW software to deduce failure sites from a user-supplied binary input string. Bottom: graphical user interface of the self-diagnosis program to identify the failures WA-2, when $N = 3$ (left) and WI-3, when $N = 5$ (right).

4% for a silica-air interface. The spurious peaks on Fig. 3 at 1534.0 and 1537.3 nm are ~5 dB less than the horizontal dotted line, which marks the level of the equivalent peaks from Fig. 2. (The proximal end of the FBG was connectorized to a 1×2 splitter and it could also contribute a weak reflection.) We index matched the distal ends of the FBGs when capturing the received signals after other failure sites on the network, achieving even better spurious peak reduction in most cases; they were often down to the noise floor. Where feasible, all stray reflections should be eliminated in installed networks.

In total, we created eight failures in the network by breaking fibers and monitoring the received spectra after each. We chose representative examples of the possibilities predicted for a three-sensor network. Table I summarizes our results, together with the decimal codes according to the theory. All instances give a perfect match. Where spurious peaks were evident in the recorded spectra, we could account for the reflections that caused them. Nearly all would be below the sensitivity limit, were a Bragg grating interrogator to be used in place of an OSA. Indeed, every spurious peak would be correctly discounted by setting a power threshold at -40 dBm.

IV. Simulation of Self-Diagnosis

The results in Section III provide clear evidence in favor of the binary state connectivity analysis of our resilient network. However, they are not, in themselves, a demonstration of self-diagnosis. Manual inference of the failure sites in a small network is straightforward, but a better means is needed when there are many sensors. We have therefore used the commercial visual programming tool LabVIEW® to deduce the sites from the patterns of received channels. Our aim was a proof-of-principle demonstrator, rather than a refined package. As operating networks would use optical receivers or FBG interrogators in place of the OSA, we did not automate the transfer of the peaks from the scanned spectra to the program.

The program has two user inputs: the number N, which network operators always know *a priori*, and the $6(N + 1)$-element received string of 1s and 0s. It converts the string into $(N + 1)$ decimal numbers, as explained in Section II. All fifteen of the three-figure decimal codes for the single failure sites modeled in Ref. [9] are stored in memory, from which a group of $(N + 1)$ decimal numbers is compiled for each single-site failure. A look-up table of decimal numbers is thus created and the input string is compared with each entry in turn until a match is found. The program also verifies the input string length for an N-sensor network and it warns if no unambiguous site identification is possible.

Fig. 4 (top) is the interior of the program, showing the two input fields on the far left. The icon "string to decimal array" converts to decimal numbers and "decimal" contains the list of failures and creates a look-up table appropriate for a network of N sensors. The sub-program ("subVI") changes the input binary string into the $(N + 1)$ decimals and the for-loop compares them with the rows in the look-up table. If a match is found, the name of the failure site is passed to the output of the loop. A case structure follows the loop to notify of a wrong string length or an unknown failure category.

The two graphical user interfaces in Fig. 4 are for WA-2 when $N = 3$, as in Fig. 2, and WI-3 when $N = 5$, as in Section II. We have also tested the program for input strings from larger networks, obtaining correct diagnoses whenever they correspond to one of the fifteen failure categories.

Our simulator is valuable for research purposes, but installed networks would normally perform their management functions, including self-diagnosis, by high-speed application-specific integrated circuits. Nevertheless, it is informative to explore how the computation times vary with N. We included a timer to measure how long the software took to identify a failure for up to forty sensors. The variation was nonlinear, growing from 0.09 s for $N = 10$ to 14.42 s for $N = 40$ and we found that the failure site chosen had almost no effect on the computation times. (The computer had Intel i3 CPU M350 dual cores, each with a speed of 2.27 GHz, and a RAM of 4

TABLE II
SINGLE FAILURES: POST-FAILURE SWITCHING REQUIREMENTS. THE FAILURE SITES ARE THE SAME AS IN REF. [9].

Failure site	Decimal code	Required post-failure connections	Pre-failure states: 3 switch changes in the SDRS	Pre-failure states: 4 switch changes in the SDRS	Pre-failure states: 5 switch changes in the SDRS
PD-m	62; 62; 56	$T_1 \rightarrow R_2$ or $T_1 \rightarrow R_3$	$T_4 \rightarrow R_2$ or $T_4 \rightarrow R_3$	$T_1 \rightarrow R_2$ or $T_1 \rightarrow R_3$	--
WD-m	31; 31; 7	$T_4 \rightarrow R_2$ or $T_4 \rightarrow R_3$	$T_1 \rightarrow R_2$ or $T_1 \rightarrow R_3$	$T_4 \rightarrow R_2$ or $T_4 \rightarrow R_3$	--
PA-m *PL-m*	53; 53; 63 63; 53; 63	$T_1 \rightarrow R_2$ or $T_4 \rightarrow R_2$	$T_1 \rightarrow R_2$ or $T_4 \rightarrow R_2$	$T_1 \rightarrow R_3$ or $T_4 \rightarrow R_3$	--
WA-m *WL-m*	43; 43; 63 63; 43; 63	$T_1 \rightarrow R_3$ or $T_4 \rightarrow R_3$	$T_1 \rightarrow R_3$ or $T_4 \rightarrow R_3$	$T_1 \rightarrow R_2$ or $T_4 \rightarrow R_2$	--
PC-m *C4-m* *C3/4-m* *PI-m*	52; 52; 56 62; 48; 56 52; 48; 56 63; 49; 63	$T_1 \rightarrow R_2$	$T_4 \rightarrow R_2$	$T_1 \rightarrow R_2$ or $T_4 \rightarrow R_3$	$T_1 \rightarrow R_3$
WC-m C1-m C1/2-m WI-m	11; 11; 7 31; 3; 7 11; 3; 7 63; 35; 63	$T_4 \rightarrow R_3$	$T_1 \rightarrow R_3$	$T_1 \rightarrow R_2$ or $T_4 \rightarrow R_3$	$T_4 \rightarrow R_2$
SU-m	63; 33; 63	Any one	All four	--	--

GByte.) Our results could be modeled by the empirical polynomial $T = 0.383N^3 - 7.513N^2 + 46.945N$, where T is in ms, and its coefficient of determination was $R^2 = 0.9998$. Although the absolute values are not those of an installed network, the trend guided our reasoning in Section V.

V. SELF-DIAGNOSTIC RECOVERY SEQUENCE

Self-diagnosis and protection switching must be coordinated to give both correct site identification and rapid post-failure service recovery. Data is lost during any recovery process and three examples from telecommunications provide a context for our results [3], [4], [15]: (i) synchronous digital hierarchy (SDH) systems with fiber spans below 1200 km perform all necessary actions within 50 ms; (ii) trans-oceanic self-healing rings take up to 300 ms, owing to the greater times of flight of the pulses; and (iii) optical meshes that use "restoration" (as distinct from protection) are less easily summarized, but, depending on the network's logical layer, recovery can exceed 1 s. Sensor applications are diverse and we do not recommend a maximum acceptable interruption. However, the modulations of (analogue) sensor signals are normally much slower than (digital) communications and so the requirements would normally be *less* stringent. A sequence of post-failure actions is proposed in this section; it ensures a short interruption during the self-diagnostic service recovery.

We make several simplifying assumptions. Only single failures are addressed and the network operates by dedicated line protection, which does not demand the control of numerous switches [10]. No amplifiers are used outside the end nodes and so we do not describe the power-up and power-down of optical pumps, which must be implemented to avoid transient spikes or the emission of powerful light from severed fibers [11]. There is one optical source per channel, rather than a shared swept-wavelength laser. Further to the description in Section III of our measurement method, channel arrivals are recorded without averaging. However, multiple measurements could be made if certainty in self-diagnosis overrides the need for fast recovery.

The topology in Fig. 1 is symmetrical and in the absence of failures full service is possible by any of the four end-to-end connections for the *sensor-modulated* channels ($T_1 \rightarrow R_2$, $T_1 \rightarrow R_3$, $T_4 \rightarrow R_2$, or $T_4 \rightarrow R_3$). We therefore assume that protection switching is "non-revertive", which means that, upon completing network repairs, no attempt is made to revert to the pre-failure switch states. Thus, protection switching in response to some previous failure could have left the end-to-end connections in any of the four combinations.

We refer to the post-failure actions as the "self-diagnostic recovery sequence" (SDRS), which is:

1. Directly after the failure, record which channels survive
2. Activate the protection switch in the RN
3. Record which channels arrive at the RN
4. Send an upstream telemetry command to the TN
5. Activate the protection switch in the TN
6. Record which channels arrive at the RN
7. Activate the protection switch in the RN
8. Record which channels arrive at the RN
9. Identify the switch states needed to recover service

At this point the switches in the RN and TN might happen to be suitably configured for service resumption. If so, only three activations will have been performed. More commonly, either one or two additional state changes are required before sensing can continue. Then, the remaining steps of the SDRS are,

10. If required, activate the switch in the RN
11. If required, send upstream telemetry to the TN
12. If required, activate the switch in the TN
13. Resume sensing operation
14. Perform the computations for self-diagnosis
15. Dispatch a repair team to the failure site

The details of the surviving channels from all four end-to-end connections are captured before service recovery and the one to be used is identified in Step 9. However, the failure site is calculated *afterwards* (in Step 14) for fear that the computation might be time consuming when *N* is large.

The failure site and the network's configuration at the time of the destructive event determine the number of switch changes in the SDRS. Table II lists all possibilities for single failures. We explain its entries by the specific example WI-m, with the X-vectors [1,1,1,1,1,1]; [1,0,0,0,1,1]; [1,1,1,1,1,1]. In accordance with (1), the positions of the *1*s indicate that only the state $T_4 \rightarrow R_3$ can recover all sensor-modulated channels. This is the entry in the third column of Table II. ($T_4 \rightarrow R_3$ also happens to be the sole connection that recovers full service after failures to C1-m, C1/2-m, and WC-m.)

The switches in a non-revertive network can be in any of the four states prior to the failure of WI-m. If they are $T_1 \rightarrow R_3$ the SDRS requires only three switch changes, as entered in the fourth column of Table II. They are $T_1 \rightarrow R_3$ ... $T_1 \rightarrow R_2$ ... $T_4 \rightarrow R_2$ ... $T_4 \rightarrow R_3$. Thereafter, all of the information for self-diagnosis has been recorded and the $T_4 \rightarrow R_3$ configuration enables all *N* channels to operate. However, a total of five changes are required if the initial status is $T_4 \rightarrow R_2$ (entered in the last column of Table II). The first three of them provide the information for self-diagnosis and the last two reconfigure the network for service resumption. The complete switching actions are then $T_4 \rightarrow R_2$ ... $T_4 \rightarrow R_3$ ... $T_1 \rightarrow R_3$ ... $T_1 \rightarrow R_2$ ... $T_1 \rightarrow R_3$ ... $T_4 \rightarrow R_3$. By similar reasoning, four switch changes are needed if the initial state is either $T_1 \rightarrow R_2$ or $T_4 \rightarrow R_3$, as entered in the fifth column.

The SRDS specifies two upstream telemetry transmissions but others might be required, for example, to confirm correct switch statuses. As a plausible worst case, if a network of 50 km length requires a total of eight end-to-end transits, the propagation delays contribute only 2 ms to the service outage. The channel recording steps and the identification of the switch states to recover service in the SDRS cause additional delays but they are not likely to exceed the times for comparable tasks in telecommunications networks. Switch activations also make a contribution. Of all entries in Table II, the greatest number of switch changes is five. As a guideline, the switches we used had activation times below 1 ms.

The total momentary interruption as a result of the SDRS is likely to be comparable to that in self-healing telecommunications networks. Even if the deductions for self-diagnosis are lengthy, they occur *after* service recovery (in Step 14). Any slight prolongation of the service discontinuity by self-diagnosis is rewarded by the considerable benefits of early notification of the failure site.

VI. Conclusion

We have experimentally demonstrated a WDM fiber bus network to interconnect sensors. It provides resilience, the ability to function despite element failures, by infrastructure duplication and protection switching. When all channels are monitored, it also exhibits important correlations between the surviving end-to-end connections after a failure and the site of that failure. This property enables self-diagnosis, a low-cost automated means to locate the affected element(s).

We have tested a representative sample of single failure sites, demonstrating the patterns of channel arrivals predicted by theory. Reflections from fiber ends can lead to multi-path transits through the network and thus spurious peaks in the received spectra. A combination of appropriate receiver power thresholds and careful refractive index matching greatly reduces their potential to cause false diagnoses. We have written simple software to deduce failure sites from the measured connections at the operating channels. It demonstrates the feasibility of automated fault localization. Self-diagnosis must be coordinated with protection switching to ensure service recovery in the shortest time and we have proposed a sequence of actions to satisfy this requirement.

Self-diagnosis augments a resilient network's functionality. By rapidly identifying failure sites it reduces repair costs and the interval during which a network is unprotected. Moreover, failure site identification is a form of sensing in its own right, which can aid the understanding of threats, especially in safety and security applications. We have thus demonstrated a network of sensors that can sense itself.

References

[1] S. Diaz, S. Abad, M. Lopez-Amo, *Fiber-Optic Sensor Active Networking with Distributed Erbium Doped Fiber and Raman Amplification*, Laser and Photon Rev., vol. 2, no. 6, pp. 480-497, (2008).

[2] M. Lopez-Amo, J.M. López Higuera, *Multiplexing Techniques for FBG Sensors*, Chapter 6 in A. Cusano, A. Cutolo, J. Albert (Eds.), *Fiber Bragg Grating Sensors: Recent Advances, Industrial Applications and Market Exploitation*, pp. 99-115, Bentham Science Publishers, 2011.

[3] R. Ramaswami, K.N. Sivarajan, G. Sasaki, *Optical Networks: A Practical Persprective*, 3rd ed., Morgan Kaufmann, 2009.

[4] A. Stavdas (editor), *Core and Metro Networks*, John Wiley, 2010.

[5] P.-C. Peng, K.-Y. Huang, *Fiber Bragg Grating Sensor System with Two-Level Ring Architecture*, IEEE Sensors J., vol. 9, no. 4, pp. 309-313, Apr. 2009.

[6] P.-C. Peng, J.-B. Wang, K.-Y. Huang, *Reliable Fiber Sensor System with Star-Ring-Bus Architecture*, Sensors, vol. 10, pp. 4194-4205, 2010.

[7] D. Anderson, L. Johnson, F.G. Bell, *Troubleshooting Optical Fiber Networks: Understanding and Using Optical Time-Domain Reflectometry,* 2nd Ed., Academic Press, 2004.

[8] Y. Wen, V. Chan, L. Zheng, *Efficient Fault-Diagnosis Algorithms for All-Optical WDM Networks with Probabilistic Link Failures*, IEEE J. Lightwave Technol., vol. 23, no. 10, pp. 3358-3371, 2005.

[9] P. Urquhart, H. Palezi, P. Jardin, *Optical Fiber Bus Protection Network to Multiplex Sensors: Self-Diagnostic Operation*, IEEE J. Lightwave Technol., vol. 29, no. 10, pp. 1427-1436, 2011.

[10] M. Schlüter, P. Urquhart, *Optical Fiber Bus Protection Network to Multiplex Sensors: Dedicated Line and Dedicated Path Operation*, IEEE J. Lightwave Technol., vol. 29, no. 15, pp. 2204-2215, 2011.

[11] O. García López, K. Schires, P. Urquhart, N. Gueyne, B. Duhamel, *Optical Fiber Bus Protection Network to Multiplex Sensors: Amplification by Remotely Pumped EDFAs*, IEEE Trans. Instrum. Meas., vol. 58, no. 9, pp. 2845-2851, Sep. 2009.

[12] M. Fernandez-Vallejo, S. Rota-Rodrigo, M. Lopez-Amo, *Remote (250 km) Fibre Bragg Grating Multiplexing System*, Sensors, vol. 11, pp. 8711-8720, 2011.

[13] M. Fernandez-Vallejo, D. Olier, A. Zornoza, R.A. Pérez-Herrera, S. Diaz, C. Elosua, C. Bariain, A. Loayssa, M. Lopez-Amo, *46-km-Long Raman Amplified Hybrid Double-Bus Network with Point and Distributed Brillouin Sensors*, IEEE Sensors J., vol. 12, no. 1, pp. 184-188, 2012.

[14] ITU-T Recommendation G.694.1 (06/2002) *Spectral Grids for WDM Applications: DWDM Frequency Grid*, 2002.

[15] ITU-T Recommendation G.841 (10/1998) *Types and Characteristics of SDH Network Protection Architectures*, 1998.