Towards Reliable Hybrid WDM/TDM Passive Optical Networks

Mozhgan Mahloo[1]**,** Abhishek Dixit[2], Jiajia Chen[1], Carmen Mas Machuca[3], Bart Lannoo[2], Didier Colle[2], Lena Wosinska[1]

[1]Royal Institute of Technology KTH, School of Information and Communication Technology, Kista, Sweden
{mahloo, jiajiac, wosinska}@kth.se

[2] Department of Information Technology, Ghent University-iMinds, Ghent, Belgium
{abhishek.dixit, bart.lannoo, didier.colle}@intec.ugent.be

[3] Technische Universität München (TUM), Germany, cmas@tum.de

Abstract

Individual users and enterprises are increasingly relying on the access to internet services and cannot accept long interruption time as easily as before. Moreover, the main characteristics of next generation optical access (NGOA) networks, such as long reach and large number of users per feeder line, turn the network reliability to an important design parameter to offer uninterrupted service delivery. In this regard, protection mechanisms become one of the crucial aspects that need to be considered in the design process of access networks. On the other hand, it should be noted that not all the users can afford to pay a high extra cost for protection and hence it is important to provide resilience in a cost-efficient way.

A passive optical network (PON) combining wavelength division multiplexing (WDM) and time division multiplexing (TDM) technologies, referred to as hybrid WDM/TDM PON or HPON, is one of the most promising candidates for NGOA networks due to its ability to serve a large number of subscribers and to offer a high capacity per user. For these reasons in this paper, we propose HPON architecture offering different degrees of resilience depending on the user profiles, i.e. partial and full protection for residential and business access, respectively. Besides, the investment cost of providing resilience for the proposed schemes is investigated considering various protection upgrade road maps.

Our results confirm that protecting the shared part of network with a large number of users is required in order to keep the failure impact at an acceptable level, with less than 5% increase of the investment cost compared to the unprotected case. Meanwhile, the proposed end-to-end protection for the business users considerably reduces the risk of service interruption for this kind of demanding users without a need for duplicating the deployment cost of an unprotected connection. Furthermore, a sensitivity analysis is performed to investigate the impact of changes in business user percentage and protection upgrade time on the deployment cost. The results may be used as an advice for a cost-efficient deployment of reliable fiber access networks.

Keywords: Resilience, Reliability, Availability, Failure impact factor, Hybrid WDM/TDM PON, Protection cost, Techno economic study.

I. Introduction

The growing number of Internet users and bandwidth driven applications, such as online gaming and high definition telepresence e.g., telemedicine, distance learning, etc., bring many challenges for the operators and force them to migrate towards new architectures. Future access networks must be able to provide high sustainable bandwidths on a per user basis while keeping the capital and operational expenses as low as possible [1]. Moreover, large coverage (i.e. long reach and large number of users

per service area) is another requirement of future access networks that makes it possible to reduce the total cost of the network by merging several central offices (COs) into single a one (referred to as node consolidation) [1]. In this regard, optical technology is one of the future proof alternatives to fulfill all the above-mentioned requirements [1].

Furthermore, the growing importance of an uninterrupted Internet access in people's daily life, along with a large coverage obtained by node consolidation, turns fault management into an important challenge for future optical access networks [2]. Individual customers are requesting the minimum interruption time while many of them cannot afford the extra cost of reliability improvement. Therefore, next generation optical access (NGOA) networks need to provide survivability schemes in a cost-efficient way [2].

The reliability requirement, however, may depend on the user profile. For example, high connection availability, e.g., greater than 99.99% (4 nines) has to be guaranteed for some business users [3], while most residential users can tolerate a lower reliability performance. It has been shown that connection availability of four nines or more cannot be achieved without protecting the full path between the CO and the user [4]. Thus, NGOA networks should also support end-to-end (E-to-E) protection for some selected (business) users when requested.

One of the most promising candidates for the NGOA architecture is a passive optical network (PON) based on the combination of the wavelength division multiplexing (WDM) technique along with time division multiplexing (TDM), namely hybrid WDM/TDM PON (HPON) [5]. WDM increases the capacity using an additional wavelength layer, while TDM improves the scalability and leads to flexible resource utilization [6].

There are several papers addressing the reliability performance of HPON. Papers [7][8] propose some new resilient architectures where fiber rings interconnect several PONs to the CO, offering protection of the network part shared by many customers. In Paper [9] splitting points are interconnected by a mesh fiber infrastructure, reducing the fiber deployment cost and allowing multiple paths from a splitting point to the respective optical line terminal (OLT) at the CO. In [4], two resilience schemes are proposed for protecting the shared part of the access network, but no cost study is presented. Paper [10] shows a fully protected PON with duplicated fibers all the way between the end users and CO. The proposed architecture offers a fast recovery, but the cost of adding backup fibers is prohibitively high. Some cost efficient end-to-end protection schemes in which optical network units (ONUs) at the users' premises protect each other via interconnecting fibers, can be found in Papers [11][12]. These schemes offer a great saving of the cost for burying redundant fibers compared to the architectures with duplicated distribution fibers [13].

None of the above-mentioned works proposes an architecture that is able to accommodate both the fully protected business users and the residential users with only protection of the shared part of the network, considering the minimized capital expenditures (CAPEX). Moreover, according to the study in [14], various migration strategies towards protected architectures can affect the total cost of ownership (TCO) which is ignored in the existing papers.

To fill this gap, this paper presents a cost-efficient architecture for HPON, supporting different levels of protection in order to satisfy availability requirements of both residential and business users. Three variants of this architecture namely wavelength selective, wavelength split and wavelength switched are considered. Two reliability performance parameters, i.e. connection availability and failure impact factor (FIF) are considered for evaluating the network resilience. .

In many cases, the initial deployments target an unprotected network in order to avoid very high investment costs, while keeping in mind a future upgrade of the network reliability performance.

Therefore, in this paper we propose an unprotected HPON architecture in a Greenfield scenario, which can be smoothly migrated towards a cost-efficient reliable architecture. Besides, the impact of protection upgrade strategies on the CAPEX is assessed by taking into account different upgrading approaches. The presented cost study is further complemented by a sensitivity analysis on the investment cost variation caused by a different density of business users per PON and the protection upgrade time.

The remainder of this paper is organized as follows. In Section II, three HPON variants are described. Section III presents the input parameters and the scenarios used in the paper. Section IV introduces cost-efficient reliable architectures compatible with any variant of HPON along with a number of options for migration towards the proposed schemes. In Section V, the reliability parameters used to evaluate the performance of each HPON variant are presented. The results of the reliability and techno-economic study along with a sensitivity analysis are presented in section VI. Finally, our conclusions are given in Section VII.

II. HPON architectures

In this section, we describe three main variants of HPON architectures. A tree topology is widely used for PON, with an OLT as the root and several ONUs as leaves (see Figure 1). In a node consolidation scenario, multiple OLTs are located at the central access node (CAN), each of which serves one HPON. Real PON implementations could include several stages of splitting points, allowing the topology to be scalable with the number of connected users. In this work, we consider two splitting stages of remote nodes (RNs) as an example to illustrate our schemes. The first RN (RN1) in a NGOA network with node consolidation is typically at the location of a CO in a legacy PON, and is connected to the OLT via a feeder fiber (FF). Through the distribution fiber (DF), each output port of RN1 goes to a second remote node (RN2) which coincides with a street cabinet and includes a power splitter (PS) as in a legacy PON. Each output port of the PS is then connected to a certain ONU by the last mile fiber (LMF). An ONU with a tunable transceiver is considered, so that a high degree of flexibility in the wavelength assignment is possible. Although the cost of this type of component is higher than a colored ONU, it can simplify the installation as well as operation (e.g. wavelength planning and management) and hence the TCO will not be affected significantly. Based on the type of RN1 configuration (see Figure 1), we define three primary variants of HPON architectures, namely wavelength selective (W-Selective), wavelength split (W-Split) and wavelength switched (W-Switch).

A. Wavelength selective H PON

As shown in Figure 1, the RN1 of a W-Selective HPON consists of a PS. Consequently, this implies a broadcast and select behaviour since each ONU has to select ultimately its assigned wavelength and time slot. This approach has the highest flexibility on resource allocation among all the HPON variants, as both wavelength and time slot can be dynamically assigned to each end user. However, it is at the expense of a high insertion loss caused by the two stages of PSs and an extra (tuneable) filter at the user side to select the particular wavelength channel.

B. Wavelength split HPON

A W-Split HPON uses an AWG at RN1. In this way, one dedicated wavelength is routed to each RN2. Although this configuration is limited in flexibility on wavelength allocation, it has a relatively long reach due to the lower insertion loss of an AWG.

C. Wavelength switched HPON

In the W-Switch HPON, active components, such as wavelength selective switches (WSSs), are installed at RN1 in combination with cyclic AWGs. WSS provides flexibility in wavelength allocation, as wavelengths channels can be switched and reallocated according to the load variations, e.g. depending on the different time of the day. However, WSS is an active component and hence a power supply at RN1 is required, which is acceptable for the considered NGOA scenario with node consolidation. Note that although WSS is more expensive and complex than AWG and power splitter, its expenses is shared among many users.

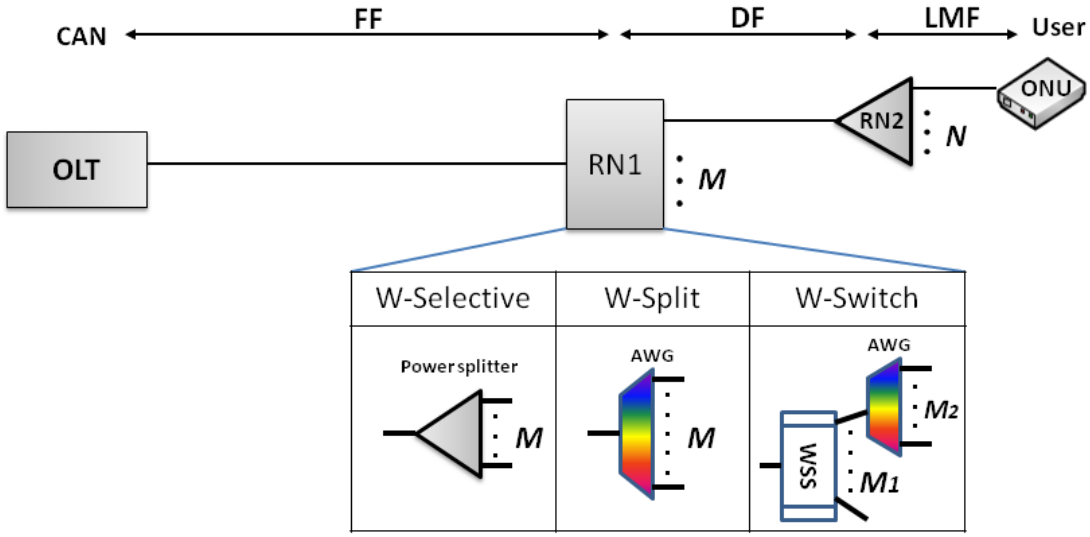


Figure 1: Basic HPON architecture with different options for RN1.

III. Input parameters and scenarios

In this paper, we focus on the dense urban area where the NGOA networks typically do not need long reach but only require a large splitting ratio. Therefore, for all the considered variants of HPON, more than 1000 ONUs are assumed to be connected to one OLT while 80 wavelength channels are used in each direction (e.g. C band for upstream and L band for downstream). To support this high splitting ratio, a booster and pre-amplifier are added at the OLT side for the W-Switched and W-Selective HPON variants to compensate for the high insertion loss. In the considered node consolidation scenario, 80 conventional COs are co-located in one CAN. Table I shows the configuration of remote nodes and client count for each variant. The reason for selecting these configurations for the splitting ratios is to have similar average bandwidth per user in all the variants. Moreover the splitting ratios should be feasible considering available devices (e.g. 1:32 power splitter, 1:40 AWG, etc).

For simplicity reason, in this study we consider a take rate of 100%. In general, the higher the take rate, the lower the cost per user.

Table I: RN configurations for different variants of HPON

HPON variants	RN1		RN2 (power splitter)	Client count
	M	components	*N*	
W-Selective	1:32	power splitter	32	1024
W-Split	1:80	AWG	16	1280
W-Switched	M1 = 1:4	WSS	32	1280
	M2 = 1:10	AWG		

The considered average lengths of the fiber sections in a HPON are presented in Table II. According to the proposed end-to-end resilience scheme a separate backup link for the DF section is not needed (see Figure 2).

Table II: Average fiber lengths in the considered dense urban area [15]

	working	Backup
Feeder fiber (FF)	6 km	11 km
Distribution fiber (DF)	1 km	-
Last mile fiber (LMF)	0.5 km	0.7 km

Input data used for the techno economic and reliability performance studies are presented in Table III. It should be noticed that the cost values presented in this paper are normalized to the common baseline of a GPON ONU and the unit is referred to as cost unit (CU).

Table 3: Considered input parameters for reliability and cost study [16].

Parameter	Cost (CU)	
Tech. Salary	1.04	
Component	Cost (CU)	Availability
AWG 1:80	24	0.9999980
AWG 1:10	3	0.9999980
Power splitter 1:2	0.6	0.9999993
Power splitter 1:8	1.8	0.9999991
Power splitter 1:16	3.4	0.9999989
Power splitter 1:32	6.6	0.9999987
WSS 1:4	263	0.9999855
OLT	463	0.9999485
Booster or Preamp	30	0.9999960
ONU with one trancever	3.2	0.9999645
ONU with duplicated tranceivers	5.8	0.9999806
Fiber (km)	4	0.9999429
Trenching (km)	900	-

IV. Reliable architectures and protection migration strategies

As it was mentioned before, an unprotected access network will not be acceptable in the future when a large number of users will be served by one OLT. Furthermore, an NGOA architecture providing different degrees of resilience is needed in order to accommodate different user profiles in the same network. On the other hand, the deployment of a new technology is very costly, especially when investment on trenching, ducts and fibers, is considered. This initial investment will be even higher if resilience has to be provided. Therefore, it is not always possible from a cost point of view to deploy a fully protected network from day one. In many cases, operators start from an unprotected architecture

and upgrade it later, as the penetration rate increases. It helps to save initial expenses and it keeps the cash flow in a good shape. However, the unprotected NGOA network should be designed considering a cost-efficient protection upgrade to maintain the total cost as low as possible.

In this regard, we propose HPON architectures with and without protection. These architectures are designed having in mind different possible paths for network deployment and protection upgrade, which are also presented in this section. The proposed survivable architectures can also be applied to networks with more than one stage of RNs based on PSs.

A. Proposed reliable HPON architectures

Figure 2 illustrates the proposed network with different levels of protection compatible with all the HPON architectures considered in this paper. The basic scheme without any protection (see Figure 2 (a)) is modified compared to the conventional deployment presented in Figure 1. The reason is that our network design takes into account facilitating an easy and cost efficient migration towards a reliable NGOA network in the future. It is in particular interesting for the case where some of the users (e.g. business users) are willing to pay extra for highly robust network access with full path protection from the OLT to the ONU. Two parallel distribution parts of the network connecting parts of RN1 (C1 and C2 in Figure 2) to the ONUs can act as the potential disjoint backup path for each other (see Figure 2 (a)). The devices at RN1 are duplicated and are connected to the FF through a 1:2 PS. In order to support the same number (*N* in Figure 2) of ONUs belonging to the TDM part of the PON and maintain the similar level of power loss as in the conventional deployment, the splitting ratio of the PS in RN2 is divided by two, whereas the number of PSs is doubled. For future protection upgrades, a limited number (denoted by "*n*" in Figure 2) of output ports of the PSs located in RN2, is reserved for E-to-E protection of some (up to *n*) selected customers. The total number of end users per PON is equal to $2*M*(N/2-n)$. The value of *n* is dependent on the percentage of E-to-E protected users. In our case we reserve ports for the business customers and we assume that the amount of business users corresponds to 5% of the total number of subscribers per PON [15].

The main goal of proposed structure is to minimize the amount of new fiber paths required to provide full protection for some selected users, which could be much more costly compared to the additional cost caused by the increased number of passive components.

Protection up to first remote node (Prot1)

In all the three considered HPON architectures, more than thousand ONUs can be connected to a single OLT through one FF, which implies the need for protection of the shared equipment and fibers in order to decrease the risk of service interruption for all the users in the same PON. From the reliability performance point of view, both the OLT and FF have high failure rates due to the use of complex active components and long fiber, respectively. Note that photonic integrated circuit (PIC) based transceivers are considered at the OLT side. This means that the whole PIC needs to be replaced even if only one of transceiver fails. Figure 2(b) shows the proposed protection (Prot1) of the shared part (i.e. OLT and FF). Compared to our basic (unprotected) scheme, the extra infrastructure and equipment needed for protection in this case is depicted in red color in Figure 2(b). In addition, the 1:M components in RN1 are replaced by the 2:M ones (i.e. 2:M1 WSS [17], 2:M PS or 2:M AWG) in order to provide connection to both the working and backup FFs. Note that the extra cost of the duplicated resources is shared by all the users connected to each PON.

End to end protection (Prot2)

For the users with high reliability requirements (e.g. business customers) protection up to RN1 may not be sufficient. A scheme, referred to as Prot2 in Figure 2(c) is proposed to offer E-to-E protection

for these demanding users. The two parallel distribution networks act as potential backup for each other, which will considerably reduce the need of additional trenching for protection.

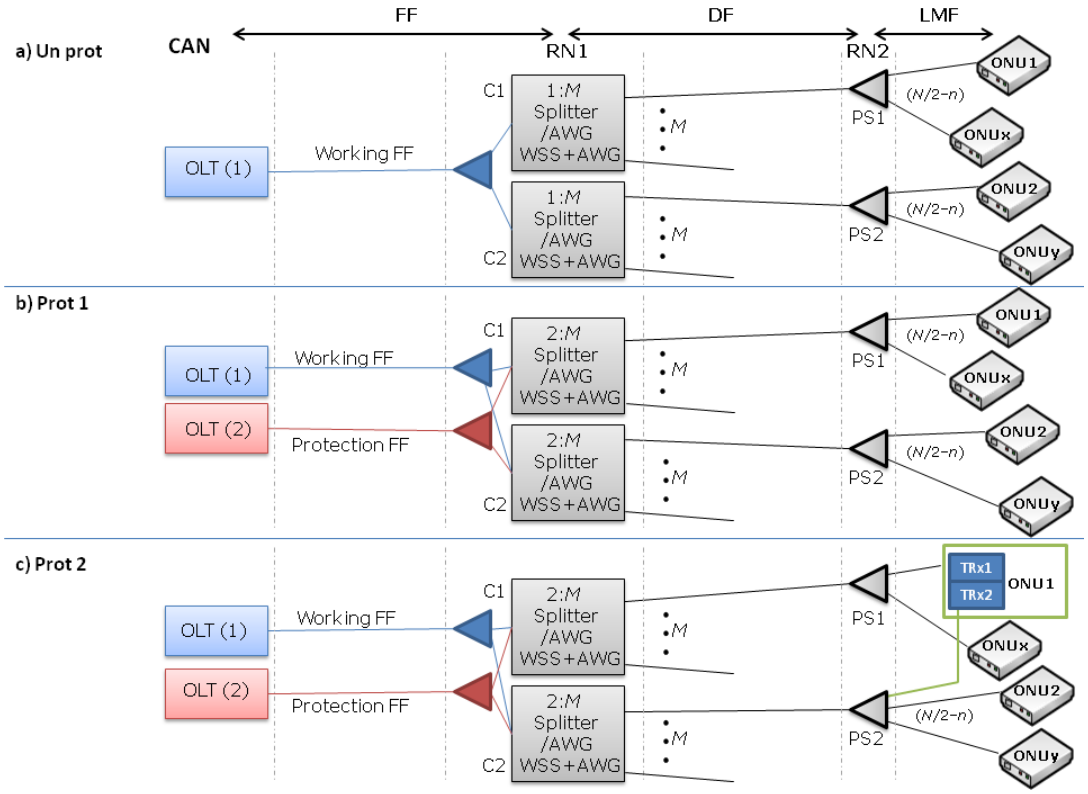


Figure 2: HPON (a) without protection, (b) with protection up to RN1 for all connected ONUs and (c) E-to-E protection for some selected ONUs compatible with all HPON variants.

To obtain an E-to-E protection, duplicated transceivers are considered at the ONU side to access both working and protection LMFs. Although it is possible to add a 2:1 coupler to connect the working transceiver at the ONU to both LMFs, type D [18] protection scheme which duplicates the optical interface in both the OLT and ONU side is preferred, due to their low availability figures as shown in table III. Furthermore, a new fiber connection for the protected ONU (see ONU1 in Figure 2(c) as an example) should be added. To decrease the new trenching required for the protection, the available ducts should be utilized, i.e. the additional connection fiber should be blown through available ducts wherever possible. Therefore, instead of connecting ONU1 and PS2 at closest RN2 with a disjoint LMF by a direct shortest path with a completely new trenching, the considered fiber route may reuse the existing trench between PS2 and ONU2 (which is the closest one to ONU1 among all the ONUs attached to PS2). In this way, a new duct would be needed only between ONU1 and ONU2, part of which could potentially be also shared with other business users to further decrease CAPEX.

Obviously, in Prot2 the users who do not need a full protection are offered the same level of resilience as in Prot1.

B. Protection upgrade paths

As indicated before, providing a certain level of protection is necessary for NGOA networks. However, network providers might prefer to start with the deployment of an unprotected network but considering the future upgrade, due to either the high initial CAPEX or low subscription rate in the

beginning. This divides the investment cost to several stages over the whole operational period, which does help cash flow, but it may lead to a slightly higher CAPEX.

In this section, we propose different protection upgrade approaches starting from a Greenfield scenario towards the proposed architecture with E-to-E protection for business users (i.e. Prot2). Figure 3 shows the three planning approaches which are further studied in the next section from a cost point of view. Operators can select one of these approaches or a combination of them depending on the specific deployment scenario.

Approach 1 (A1): This approach includes three steps of deployment. In the first step (denoted as S1 of A1 and referred as A1:S1), providers will deploy an unprotected access network. Since the penetration rate grows gradually, after a while the need of protection at least in the shared part will push the provider to offer resilience till RN1 (which is referred to as the second step, i.e. A1:S2). This level of protection is necessary in order to prevent that a large number of customers will be out of service at the same time. Finally, as the third step (i.e. A1:S3) protection of the distribution part of the network is offered on a per-user basis as soon as a business customer, request for reliability performance improvement

Thus, the operator will first deploy the unprotected network shown in Figure 2 (a) followed by two steps of protection upgrade in the later stages (see Figure 3).

Approach 2 (A2): Due to the high cost of the civil work (900 CU per kilometer for trenching), sometimes providers prefer to do the planning in one step and try to avoid double construction work later. This will lead to a higher investment cost in the first year, but might decrease the total CAPEX. So, in this approach we consider the transition from a Greenfield directly to Prot1 (referred as the first step and denoted as A2:S1), having the possibility of adding E-to-E protection for the business users in the future if required. Thus, A2 is a two-step approach taking into account one step of protection upgrade when requested. This approach is more logical in case a provider has a monopoly and every user in the region has to switch to its network eventually. As the second step (A2:S2), we consider upgrading the network reliability for the business users in the service area. The protection upgrade in A2 is done at the first step, and the amount of required digging for the backup feeder fiber could be less than A1**.** The main reason is that in some locations, especially in densely populated areas, it might be restricted to dig the ground at some points of time due to the circumstances related to the municipality (e.g., ongoing construction works).

Approach 3: If the operator knows in advance the location and the number of all residential and business users in its network, it might be more beneficial to deploy a reliable NGOA network in a single step (A3), from Greenfield directly towards Prot2.

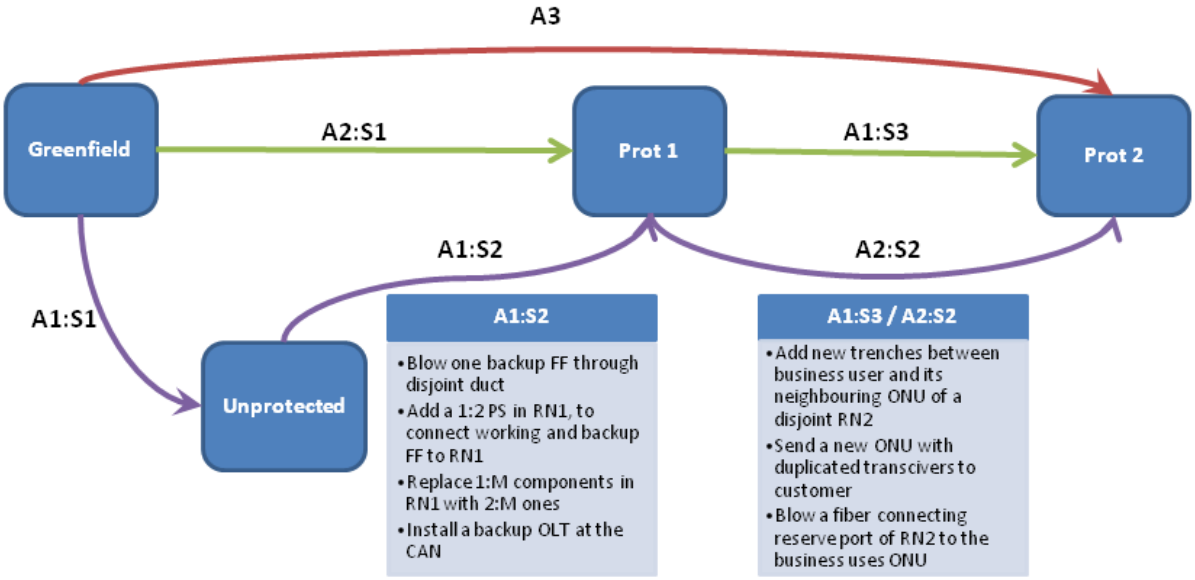


Figure 3: Protection upgrades paths

V. Performance parameters

In this section, we present the performance parameters used for reliability analysis.

A. Connection unavailability

Asymptotic unavailability is defined as the probability that a component/link is inoperable at an arbitrary point of time [19]. Connection unavailability means the probability that a logical connection (e.g. the one between the OLT and ONU) is disconnected and can be calculated using the models in [11].

The minimum required value of connection unavailability depends on the network operators' policy and the customers' profiles. However, reducing connection unavailability in NGOA below 10^{-5} does not make any improvement, since the reliability performance of aggregation networks will limit the overall connection unavailability [20].

On the other hand, unavailability below 10^{-4} is not accessible without providing an E-to-E protection, which might be too expensive for residential users [4]. These users may accept to experience longer interruption times in order to avoid a higher subscription fee. Therefore, residential customers can be served with a relaxed unavailability, i.e., higher than 10^{-4}. On the other hand, business users may have high reliability requirements [3] and hence they would pay more to get the guarantee for connection unavailability less than 10^{-4}.

B. Failure Impact Factor (FIF)

Besides connection unavailability, network operators are also interested in the impact of a failure, i.e. a risk that a large number of customers will be affected. For instance, if an OLT (at the CAN) fails it would impact all customers in the PON whereas a problem at an ONU (at the user end) would only affect one customer. Typically, network operators are more concerned about a single, high impact failure than many small uncorrelated events (with the same total impact), since a single high impact failure does more harm to the company image and could lead to negative press releases. In this regard, we define a new reliability performance parameter, namely failure impact factor (FIF), which takes

into account two important parameters relevant to resilience. One is the failure penetration range (FPR), i.e. the number of users simultaneously affected when a fault occurs in a certain component (link), and the second one is the unavailability (*U*) of such component (link). FIF is given as:

$$FIF_{component/link} = FPR \times U \qquad (1)$$

where: FPR = Number of customers affected by a failure

U = Unavailability of a component/link

The FIF of a connection, consisting of a sequence of components (e.g. OLT, ONU, RN1, RN2) and/or links (e.g. FF, DF, LMF) is defined by:

$$FIF_{connection} = \sum FIF_{component/link\ i} \qquad (2)$$

It can be clearly seen that for a larger value of the FIF for either a component/link or a connection, a higher number of users may simultaneously experience a service interruption. If the unavailability of a certain component/link is 10^{-4}, a FIF of 0.1 indicates that 1000 customers will be affected by the failure of this component. Based on the discussions with the operators in the European FP7-OASE project, we believe that a FIF of 0.1 should be considered as an upper bound for this metric [4].

VI. Performance evaluation

This section performs an evaluation of the connection unavailability, the FIF and the deployment cost, along with a sensitivity analysis.

A. Connection unavailability

Figure 4 (a) compares the connection unavailability of the three architectures presented in Figure 2 and considering all the three HPON variants, i.e. W-Selective, W-Split and W-Switch. The results for Prot2 show the connection unavailability offered to the business customers (i.e. with E-to-E protection), while the bars related to the Prot1 and Un Prot correspond to the unavailability for all types of users.

Generally the results for connection unavailability are similar for all considered variants of HPON. However, the W-Switch HPON has slightly higher connection unavailability due to the active component located in RN1. Adding protection up to the RN1 can reduce unavailability to an acceptable level for residential users, though it is not satisfactory for the business customers. Using the Prot2 scheme, the connection unavailability of business users decreases by one order of magnitude compared to Prot1.

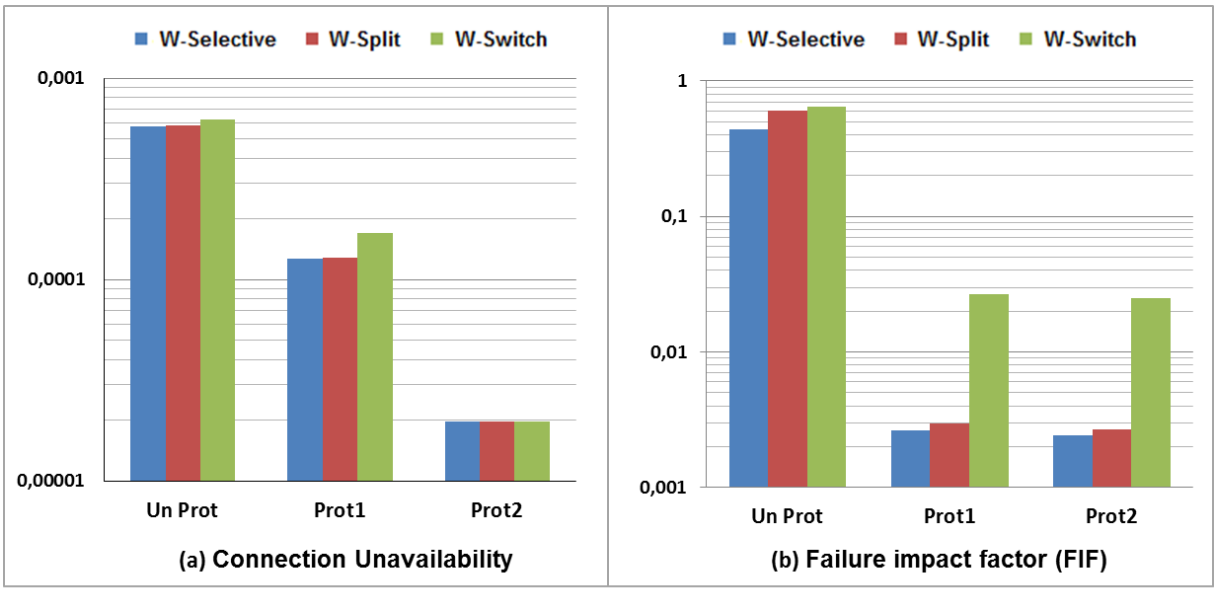


Figure 4: Connection unavailability (a) and FIF (b) for various HPON architectures.

B. Failure impact factor (FIF)

The calculated FIF values are shown in Figure 4 (b). It can be seen that in all the cases, the FIF values can be considerably reduced by both Prot1 and Prot2. A FIF less than 0.01 can be obtained for both the W-Selective and W-split options, while the W-Switch HPON shows lower improvement due to the higher unavailability of active components located in RN1. However, even in the W-Switch case the achieved FIF values are in the acceptable range (i.e. <0.1). The FIF value of Prot2 is very similar to Prot1, since protecting a few business users in the distribution part of the network has a small impact on the failure penetration range. It should be noted that the number of users affected by a single failure in the distribution part of the network is much lower than the failure of either FF or OLT, and hence adding resiliency in the distribution segment of the network will not improve the FIF.

C. Deployment cost (CAPEX)

CAPEX considered in this paper includes not only the cost of components, but also expenses related to the fiber infrastructure and installation. It is calculated according to the model presented in [21]. Figure 5(a) shows the CAPEX divided to component and infrastructure cost for approach three as an example. This figure gives a general view of the fact that how dominant is the infrastructure cost in network deployments. As expected the W-Switched HPON has the highest component cost due to the usage of WSS, but this difference is negligible as it is shared by more than 1000 users. The W-Split HPON is the most expensive architecture due to the smaller splitting ratio of the PS in RN2 (1:8) which leads to a larger number of required fiber paths in the distribution part of the network and higher infrastructure cost. It can be also seen that the W-Switch variant is slightly cheaper than the W-Selective one. This is caused by a larger client count in the W-Switch HPON than the W-Selective HPON. Figure 5(b) and (c) present the CAPEX per user considering the three protection upgrade paths for business and residential customers, respectively.

The CAPEX contributions of the three steps in each approach are depicted in Figure 5(b) in blue, red and green where applicable. Since the residential customers do not have E-to-E protection, only two steps (colors) appear in Figure 5 (c).

In general, more intermediate steps will lead to a higher total CAPEX, though less initial investment is needed from the operator point of view. Having several steps of deployment will increase the number

of travels to/from the locations leading to a higher installation cost. It might also involve additional devices for intermediate steps, such as 1:M devices in RN1 for the unprotected cases, which in turn increases the component related CAPEX.

A considerably low extra cost for offering protection up to RN1 compared to the unprotected case (i.e. around 2 CUs per user) (A1:S2) justifies the effectiveness of this option. The green part of the bars depicted in Figure 5 (b) represents the extra cost of E-to-E protection that should be paid by business users. By adding full protection, CAPEX is nearly doubled for business users compared with the residential ones with protection up to the RN1, mostly caused by new digging and trenching expenses. This fee needs to be paid for a considerable improvement of the connection availability.

It should be mentioned that the CAPEX for the unprotected scheme presented in Figure 2 (b) is 5% more expensive than the conventional architecture depicted in Figure 1, while the cost of adding full protection for the selected users is reduced nearly twice using the proposed unprotected architecture.

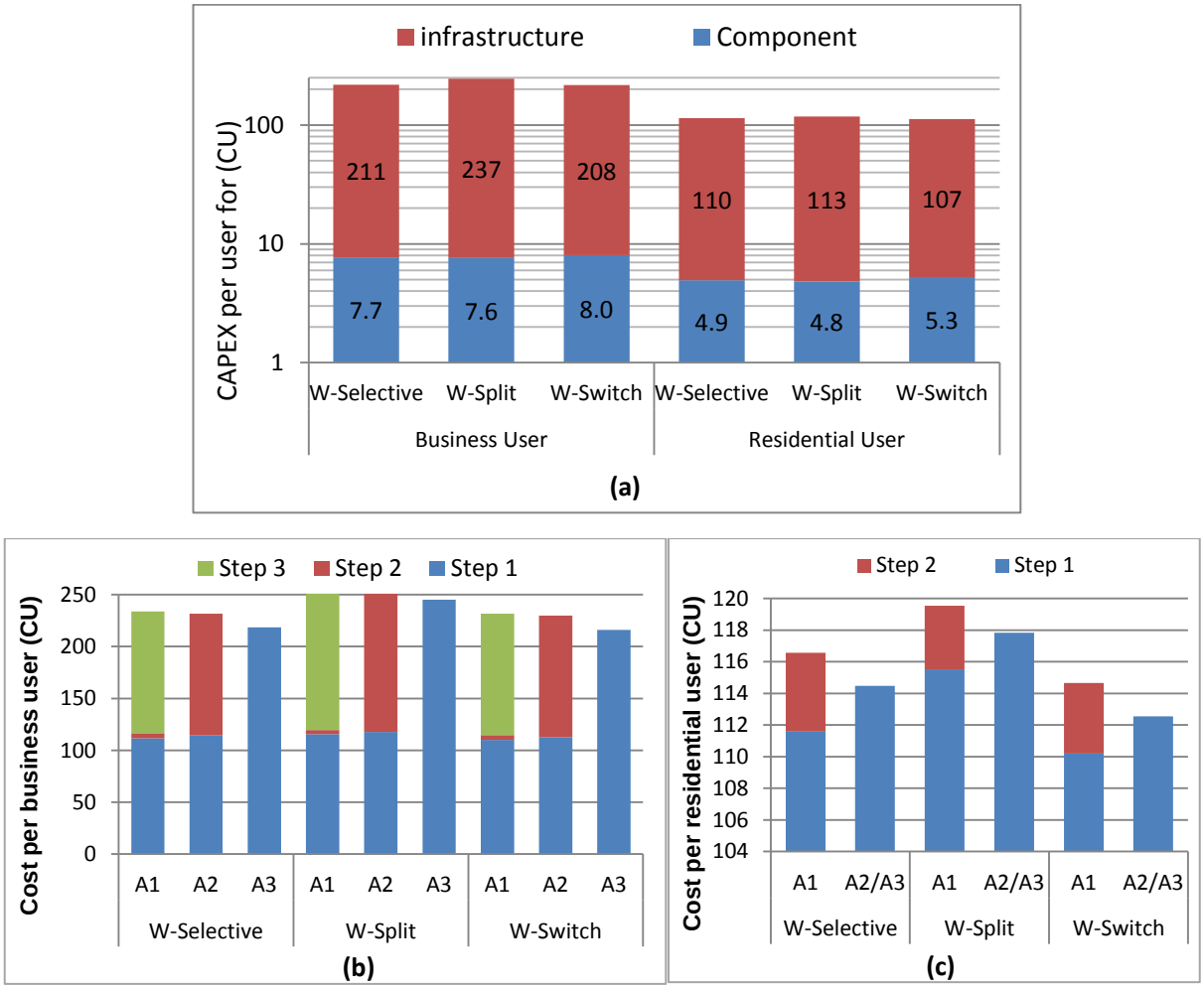


Figure 5: (a) Detailed CAPEX per user considering A3, cost per (b) Business user and (c) Residential user for HPON architectures considering three protection upgrade approaches

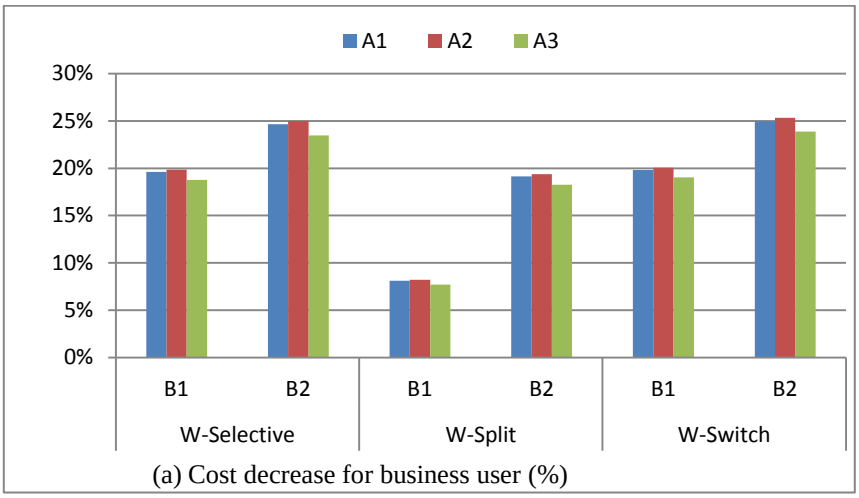
D. Sensitivity analysis

In this section, we perform a sensitivity analysis on two input parameters used for the cost studies in the previous section, which could vary according to the geographical region, financial conditions or operator policies. It can help to investigate their impact on the deployment cost of fiber access networks.

Business user density

The density of business users varies depending on the region, which can affect the investment cost for protecting HPON. To see this influence, the cost variation caused by changing the percentage of business users per PON is evaluated and presented in Figure 6 (a). The percentages of business users for cases B1 and B2 are assumed to be 10% and 15%, respectively. Note that all the reliability performance and the cost results presented in the previous sections are obtained assuming 5% of business customers' density, which is used as the reference case for this section. Figure 6 (a) shows the decrease of CAPEX per business user for B1 and B2, in percentage compared to the benchmark.

The results show that in all the considered approaches increasing the number of business customers lead to a considerable reduction of the investment cost for protection, given that the disjoint last mile trenching cost can be shared among a larger number of users. For example expanding the business users percentage per PON from 5% to 10%, leads to nearly 20% reduction of CAPEX for business customers, while the same amount of rise from 10% to 15% will only decrease investment cost by 5%. Note that the increase of the enterprises (n) in the region drops the client count ($2*(N/2-n)$) slightly. Therefore, the CAPEX related to the residential users only negligibly increases, which is not shown here.



(a) Cost decrease for business user (%)

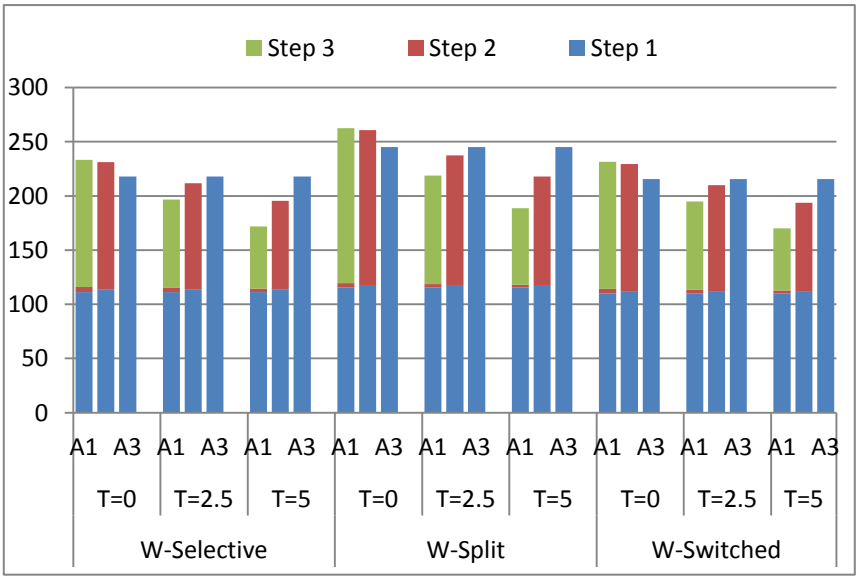


Figure 6: Deployment cost of HPON variants for business users considering various (a) business user percentage, (b) protection upgrade time per PON.

Protection upgrade time (T)

The time frame in which the operator decides to upgrade the network reliability performance can play an important role for the CAPEX. The impact of different time periods on the deployment cost is evaluated for each migration approach. We define *T* as the time between each two steps of the upgrading process. For example, considering *T* equal to 5 years in A2, it takes 5 years before deployments of Prot2 from the starting point, while in A1 the deployment is finalized in 10 years (Prot1 after 5 years and 5 years more to deploy Prot2). To see the influence of time on the cost a 7% decrease per year is considered for the equipment cost, as well as 3% increase per year for the technician's salary that will lead to the higher cost of installation and trenching. It should be noted that a certain amount of money today has different buying power than the same amount of money in the future []. This fact is reflected by adding a discount rate of 10% per year to calculate net presented value (NPV) of the CAPEX when investment is divided in several steps during a time period.

This impact is shown in Figure 6 (b) by calculating the total CAPEX per business user for all three planning approaches considering T equal to 0, 2.5 and 5 years.. It can also be seen that the number of steps is important considering the price fluctuations. Investment cost for A3 does not change by T, as it only has one step done in the first year. Regarding the deployment with more than one step i.e. A1 and A2, the longer the investment time, lower investment cost is needed considering 10% discount rate per year for the investment. It is shown that considering the cost fluctuations in the input values and NPV, dividing the investment to several steps lead to a lower investment. Therefore, A1 with three steps is the cheapest option in a long run. Moreover, it can be also seen that the longer network planning time (T) leads to the lower total CAPEX. Therefore, the proper time plan of deployment can lead to huge savings for the operators.

VII. Conclusions

In this paper, we propose novel architectures for three variants of HPON where different degrees of the reliability performance can be reached in order to meet distinct availability requirements of residential and business users. The main principle for our design of resilience is to offer a cost efficient protection upgrade. A comprehensive cost study is presented to show the investment needed for various user profiles considering three migration-planning approaches towards a reliable network.

Our assessment of cost and reliability performance clearly confirms the benefits of providing protection up to the first remote node with very low extra investment and significant improvement in resilience, especially failure impact is reduced more than 10 times compared to the unprotected case. Moreover, an E-to-E resilience scheme is introduced having in mind minimizing amount of required new equipment and infrastructure in the field for the business users. According to the results, providing full protection by investing less than twice of the CAPEX of an unprotected network, leads to a considerable improvement in the connection availability of the enterprises.

The expenses of providing E-to-E protection using our scheme are related to the density of business users in the service area. According to our cost analysis, it will be cheaper to offer full protection in regions with a larger amount of business users, due to the higher possibility to share infrastructure.

Besides, we also analysed different approaches for the protection upgrade that operators can follow. The results show a clear benefit when network planning is done having in mind the future protection upgrades, which leads to a decrease in the investment cost. Additionally, it has been shown that the time between two steps of network deployment will affect the capital expenditures. It is demonstrated

that the longer the protection deployment time the higher the total CAPEX. This confirms the importance of the right deployment plan.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community's Seventh Framework Program (FP7/2007-2013) under grant agreement n° 249025 (ICT-OASE) and n° 318137 (ICT-DISCUS).

References

[1] D. Breuer et al, "Opportunities for next generation optical access", IEEE Communications Magazine, Vol. 49, pp. 16-24, 2011.

[2] R. Hülsermann et al, "Impact of network reliability on network costs in next generation access networks", International Conference on Transparent Optical Networks (ICTON), 2010.

[3] Carrier-Class Availability for Enterprises, Alcatel technology whitepaper, "http://www.adventus.lt/lt/products/datacom/files/T0212-Availability-EN.pdf",

[4] A. Dixit et al, "Efficient protection schemes for hybrid WDM/TDM passive optical networks", IEEE International Conference on Communications (ICC), Workshop on New Trends in Optical Networks Survivability, 2012.

[5] K. Grobe et al, "PON in adolescence: from TDMA to WDM PON", IEEE Communications Magazine, Vol. 46, pp. 26-34, 2008.

[6] A. Dixit et al, "Flexibility evaluation of hybrid WDM/TDM PONs", IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2011.

[7] D. M. Seol et al, "Cost-effective protection in long-reach hybrid PON", European Conference on Optical Communication (ECOC), 2010.

[8] B. Mukherjee, "Reliable architectures for next generation broadband access networks (RANGBAN)",Asia Pacific Optical Conference (APOC), 2008.

[9] L. D. Truong et al, "Impact of mesh topology in cost reduction of survivable hybrid WDM/TDM PON networks", Symposium on Information and Communication Technology (SoICT), 2012.

[10] D. M. Seoll et al, "Passive protection in a long-reach WDM/TDM PON", International Conference on Optical Internet (COIN), 2010.

[11] J. Chen et al, "Analysis of protection schemes in PON compatible with smooth migration from TDM PON to hybrid WDM/TDM PON", Journal of Optical Networking, Vol. 6, pp. 514-526, 2007.

[12] J. Chen et al, "A novel protection scheme for a hybrid WDM/TDM PON", proceeding SPIE , Network Architectures, Management, and Applications, Vol. 6784, 2007.

[13] J. Chen et al, "Scalable passive optical network architecture for reliable service delivery", IEEE/OSA Journal of Optical Communications and Networking, Vol. 3, pp. 667-673, 2011.

[14] C. Mas Machuca et al, "Cost-efficient protection in TDM PONs", IEEE Communications Magazine, Vol. 50, pp. 110-117, 2012.

[15] "http://www.ict-oase.eu/public/files/OASE_D5.1_WP5_DTAG_rev2012.pdf", OASE Project D5.1: Overview of methods and tools, September 2010.

[16] "http://ec.europa.eu/information_society/apps/projects/logos/5/249025/080/deliverables/001_OASED421WP4UEssex31Oct2011V10.pdf", OASE Project, D4.2.1: Technical assessment and comparison of next-generation optical access system concepts, October 2011.

[17] Y. Akiyam et al, " Optical cross-connect using wavelength selective switches", US Patent 7 933 519, Apr. 26, 2011.

[18] Broadband optical access systems based on passive optical network (PON), ITU-T rec. G983.1, 1998.

[19] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M.Jaeger, "General availability model for multilayer transport networks", in Proc. 5th Int. Workshop on DRCN, Oct. 2005, pp. 85–92.

[20] M. Vogt et al, "Availability modeling of services in IP networks", International Conference on Design of Reliable Communication Networks (DRCN), 2003.

[21] M. Mahloo et al, "Protection cost evaluation of WDM-based Next Generation Optical Access Networks", Elsevier Optical Switching and Networking (OSN), Vol. 10, pp. 89-99, 2012.