Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 6250893, 13 pages
https://doi.org/10.1155/2017/6250893

Research Article

Prioritising Redundant Network Component for HOWBAN Survivability Using FMEA

Cheong Loong Chan,[1] Sheng Chyan Lee,[1] Kee Choon Yeong,[1] and Su Wei Tan[2]

[1] *Universiti Tunku Abdul Rahman, Kampar Campus, 31900 Kampar, Perak, Malaysia*
[2] *Multimedia University, 63100 Cyberjaya, Selangor, Malaysia*

Correspondence should be addressed to Cheong Loong Chan; chancl@utar.edu.my

Received 14 July 2016; Accepted 13 October 2016; Published 11 January 2017

Academic Editor: Leyre Azpilicueta

Deploying redundant component is the ubiquitous approach to improve the reliability and survivability of a hybrid optical wireless broadband access network (HOWBAN). Much work has been done to study the cost and impact of deploying redundant component in the network but no formal tools have been used to enable the evaluation and decision to prioritise the deployment of redundant facilities in the network. In this paper we show how FMEA (Failure Mode Effect and Analysis) technique can be adapted to identify the critical segment in the network and prioritise the redundant component to be deployed to ensure network survivability. Our result showed that priority must be given to redundancy to mitigate grid power outage particularly in less developed countries which is poised for rapid expansion in broadband services.

1. Introduction

Statistics from ITU indicate conclusively that there is continued rising trend in demand for higher data transmission rate and wireless mobility [1]. While wireless network can furnish the required mobility, it is constrained by the scarce favorable radio spectrum. On the other hand, optical fiber network is able to fulfill the vast bandwidth desired but unable to quench the ongoing plea for mobility. Studies have suggested that a hybrid optical and wireless broadband access network (HOWBAN) that incorporates a high speed optical fiber network at the back end and a wireless mesh mobile network at the front end would be primed to provide a compromise to the market pressure [2, 3].

Minimising the network deployment cost is essential for successful acceptance of HOWBAN [4]; however the ability to ensure that the network can continue to function during failure is equally important [5]. The introduction of high bandwidth technology such as NGPON, LTE-A, and 5G with 10 times higher bandwidth and in particular IEEE802.11ac will increase the number of clients that can be served by the nodes in HOWBAN. The failure of the network component will affect more mobile clients (MC) compared with the previous technology. Reliability and survivability of HOWBAN are thus becoming more critical and urgent.

We have shown in our previous work that increasing the number of potential sites for wireless access points (WB) has little impact on the deployment cost which is dominated by trenching cost [6]. The simulated result obtained indicated that full survivability cannot be ensured by merely optimising the cost of a wireless mesh network (WMN). Node failures in the WMN need to be addressed in order to improve network survivability. In view of the growing trend in network data rate and adoption of mobile communication services, unrecovered node failure will affect significantly both network operators and users. The network operators have to guarantee that the level of connection availability adhered to the service level agreement (SLA) [7] as required by the respective national telecommunication regulator [8] and retain client loyalty so as to maintain and improve their ARPU (average revenue per user). For the users, particularly those in industries relying on ICT services for mobile financial transactions, network failure will create loss in revenue [9, 10].

Deployment of redundant components is the ubiquitous practice in improving the reliability and survivability of a network due to node and link failures. Numerous studies have been done to evaluate the impact of node failure and strategies to resolve the problem. However, to our knowledge no formal tools have been used to enable the evaluation and decision to prioritise the deployment of redundant facilities in the network. Failure Mode Effect and Analysis (FMEA) tools which are commonly used in the manufacturing sector are a quality method designed to anticipate potential failure modes and prevent failures. In this paper we adapt the Failure Mode Effect and Analysis (FMEA) tools to identify the potential failures in the network infrastructure and weigh the impact of the failures for prioritising the redundant facilities to be deployed. The intrinsic feature of FMEA systematic technique to assess risks and preventive measures to ensure reliability is deemed fitting for the proposed evaluations of the hybrid optical wireless broadband access network (HOWBAN).

The rest of the paper is arranged as follows. In Section 2 of this paper, the architecture of HOWBAN, typical network failures, and various works that have been attempted to minimize cost of network redundancy in order to preserve survivability of HOWBAN will be presented. The Failure Mode Effect and Analysis (FMEA) strategy is deliberated in Section 3. Section 4 examines the results obtained from FMEA process. The pros and cons of using FMEA techniques and future work are discussed in the conclusion in Section 5.

2. HOWBAN Architecture and Network Failures

The architectures of HOWBAN incorporating a passive optical network (PON) and a wireless mesh network (WMN) are as shown in Figure 1. The ubiquitous infrastructure based and ad hoc wireless mesh network are depicted in Figures 1(a) and 1(b), respectively. The regulatory permission to operate wireless mesh network in the license-free 2.4 and 5 GHz industrial, scientific, and medical (ISM) band is a positive factor that has spurred the widespread adoption of the 802.11 Wi-Fi technologies in wireless mesh networks. The infrastructure based WMN front end using Wi-Fi technology is assumed in this paper.

Wireless mesh networks are characterised by their short deployment time and relatively low implementation cost compared to cabled network. The communication range of a wireless mesh network can easily be extended and it has the capability for self-healing. For the infrastructure based wireless mesh network shown in Figure 1(a), the mobile clients (MC) will connect to the Internet via a wireless access point (WB) within its best communication range. The data received from MC is relayed by the host WB to a gateway router (GW). Since the access points (WB) and gateway routers (GW) in the network are connected in a mesh topology, the range of communication of a WB can easily be extended by allowing their traffic to be relayed or "hopped" to neighbouring WB. This multihop feature enables the communication range of a WB to be extended easily. The self-healing capability is achieved by rerouting traffic to alternative neighbouring WB if the intended link failed.

Gateway routers (GW) are typically sited within communication range of several WB and are tasked to link the WB connected to them to the optical network. Each gateway router is attached to an Optical Network Unit (ONU) which converts the electrical signal received to optical form. Data from the source WB continued its path as optical signal using the distribution fiber (DF) to the optical splitter or remote node (RN) using time division multiplexing (TDM). The passive optical splitter acts as a power combiner to assemble the upstream data from various ONU and forward it via the feeder fiber (FF) to the Optical Line Terminal (OLT) which is conventionally sited at the central office (CO). The data received by the OLT is presented to the Internet via the terrestrial cabled network.

On the reverse or downstream path, data from the Internet will be returned to the source WB via the FF, optical splitter, DF, ONU, and GW. The OLT, feeder fiber, optical splitter, distribution fiber, and the ONU form a passive optical network (PON). The optical splitter serves to divide the optical signal power from the feeder fiber into multiple and equal but lower power signals to the distribution fibers. Duplex communication where upstream and downstream signals can be transmitted simultaneously over the same fiber is adopted in the PON using wavelength division multiplexing (WDM) by deploying different laser wavelength for the upstream and downstream path. A typical uplink laser signal from the ONU to the OLT is transmitted using 1310 nm light wave while downlink signal from the source OLT to the ONU is achieved using a wavelength of 1490 nm. Each distribution fiber is terminated with an ONU which converts the optical signal to the electrical signal and fed to the GW associated with it using time division multiple access (TDMA).

2.1. Network Failures. The 1 : 1 redundant network offers the simplest and most effective solution as insurance to network survivability as it can drastically reduce the recovery and down time but will attract exorbitant cost and is not economical [11]. As redundancy cannot be averted to maintain network survivability, various attempts have been done to reduce network component redundancy. This section will review the work that has been done to resolve the failure in the backhaul and front end of HOWBAN.

2.1.1. Backhaul Failures. Various parts of a PON including outside plant can fail due to mechanical, optical, or electrical faults [12]. Most of the investigations on optical network node failures are done on the impact of equipment failure and fiber cut. The objectives revolve around protection strategies and minimising the physical redundant system to ensure network can continue to operate by providing alternative or multiple paths for data from the failed node or fiber break. Techniques to ensure reliability of the optical backhaul include the use of optical switches with redundant fiber or equipment [13] and diversion of traffic of ONU attached to failed distribution fiber to neighboring ONU [2, 14, 15].

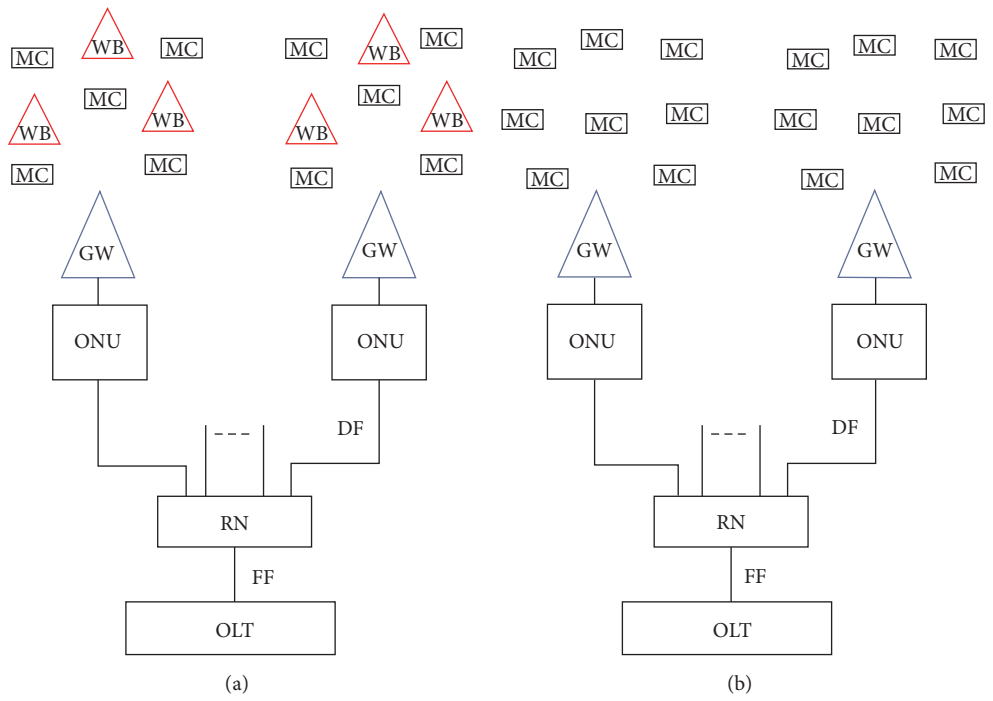

Figure 1: HOWBAN architecture: (a) infrastructure based WMN; (b) ad hoc WMN. MC: mobile clients; WB: access point; GW: gateway; ONU: Optical Network Unit; DF: distribution fiber; RN: optical splitter; FF: feeder fiber; OLT: Optical Line Terminator.

In [16] each parcel of the hybrid network consists of an OLT and a RN servicing several ONU. Each ONU is attached to a GW linked to their respective WB. A backup ONU is assigned to each parcel which is connected to its peer in at least another parcel via an optical fiber. When discontinuity due to failure in either DF, RN, FF, or OLT in a parcel occurred, data from this parcel will be routed using the backup ONU to its peers in other parcels. The backup ONU in the new parcel will then distribute the data received wirelessly to all GW which are connected to live ONU and OLT. In this case, survivability is achieved using the backup ONU and a redundant fiber connected to neighbouring backup ONU.

In the optical access network, link-level reliability can be ensured easily by using tree or trunk protection mechanisms which also minimise the number of redundant pieces of equipment deployed [12]. Optical switches are used to divert the data to redundant fiber when traffic flow is blocked due to failure in optical path or ONU [5]. Fiber cut protection generally required the use of an alternative fiber path. The alternative path can be either a redundant fiber or a neighbouring fiber with spare capacity or running on a different laser wavelength [5, 17–19]. In [20], the distribution fiber cut protection is achieved wirelessly by routing traffic from GW with broken optical path to neighbouring GW with spare capacity and attached to working optical path. The proposed scheme can avoid the use of redundant fiber assuming an alternative wireless route or GW with sufficient spare capacity is available but this approach will complicate the design of the wireless mesh network.

Deploying redundant OLT is prevalent in OLT protection although various proposals have been made to reduce the number of redundant OLTs. A $1:N$ OLT protection scheme by using a redundant OLT and an optical switch is proposed in [21]. Data from any failed OLT will be switched to the spare OLT. This approach reduces the number of redundant OLTs but nevertheless still required the use of at least one redundant OLT. It will also be unable to handle multiple OLT failure. A combined ring star fiber connectivity topology to reduce the number of redundant OLTs for protection is proposed in [22]. In [23], the load from the failed OLT is distributed to other working OLTs using optical control unit and optical switch. Although no dedicated redundant OLT is deployed, there is still the inevitable and ineluctable requirement of nondedicated OLT to protect OLT failure.

A survey done by China Telecommunication as reported in [12] shows that 80% of the faults in the outside distribution network are due to mechanical connectors which can be avoided by reducing the use of mechanical connectors and adopting appropriate good practice during installation. Equipment failure is due mainly to circuit components and power supplies.

The survey also indicated 13% of the network failures are due to configuration error created by the users and 26% of the failures are at the management platform. These problems can be solved using software define networking which aims to simplify network management and configuration through isolation of management of the control logic and networking devices that forward the traffic in the network [24, 25].

2.1.2. Front End Failures. Typical failure in wireless front end can be due to atmospheric attenuation and interference, network congestion, or equipment failure [26]. Failure in

WB/GW segment will disrupt the link path for data flow resulting in potential changes in network topology for routing and creating network congestion [27]. In the worst case, the network survivability may not be maintained. The use of multiple radios provides more radio channel for communication thus enabling higher data capacity and throughput. The extra radios may provide wireless backup link for failure of radio in the main path thus improving the robustness of the network [28]. This strategy will increase the capital expenditure but it is still viable due to the drop in the cost of radio hardware [28]. However, studies have shown that employing more than three radios will be counterproductive to the attempt to improve connectivity due to the excessive interference created by the additional radios [29, 30].

Deployment of more WB nodes inevitably will increase the coverage area and more choices of transmission paths that lead to improving network resiliency while reducing path loss will improve the network throughput [31]. The drawback is that the hop count will escalate in proportion to the WB and will incline to make the link delay intolerable [31, 32]. Authors in [31–33] reported some algorithms such as minimum hop, shortest path, delay aware, and least state prediction to optimise the link latency. This approach will increase the complexity of the algorithm which can be reduced by optimising the siting of redundant WB and GW to maximise the number of alternative paths to reroute data from failed nodes without creating undue delay.

2.1.3. Our Contribution. The work done so far indicated the broadband access network operators have full control of all the resources and solutions to resolve the failures in the network except for failures due to grid power outage which is usually under the purview of the electricity utility providers. Most studies are aimed at evaluating the impact of providing redundant resources in different segments of the HOWBAN on network availability and survivability. Our work differs in that we identify and prioritise the critical segment and the redundant component that need to be deployed to ensure network survivability.

3. FMEA Method for HOWBAN

Deploying redundancy in the network will inevitably incur additional CAPEX and OPEX [12] but it is essential to mitigate the indirect cost of network failure in terms of noncompliance with service level agreement and loss of revenue from related services. FMEA technique can be used to help reduce the cost of redundancy by identifying and prioritising the critical redundant component needed in the network.

FMEA is employed in engineering to specify, discover, and remove predictable and plausible faults from a system in order to improve its reliability [34–39]. Reliability is a measure on the probability of a system or in this case a network, accomplishing its planned function in the required duration and operating environment [34]. FMEA helps to analyse and overcome different failure modes that may affect the reliability of a system or in this instance the hybrid optical wireless broadband access network prior to its implementation [34]. Failure mode and failure effects are two key evaluation criteria used in FMEA. Failure modes are ways where the network fails to provide reliable and uninterrupted service to its clients. The failure modes may be due to failure of network components, intermittent operation, and partial or total loss of service [40]. Failure effect focuses on the effects of failures on the network function. The FMEA tools provide a foundation to identify potential failure modes due to deficiencies in the network. Typical FMEA evaluation forms are given in [40, 41]. In this paper, FMEA is used to evaluate the reliability of both the functional and hardware components of a hybrid optical wireless broadband access network.

FMEA hinged on Risk Priority Number (PRN) for root causes of the potential failure modes to appraise the risk of the system and prioritise the actions that need to be taken [34]. A Risk Priority Number (PRN) is derived for each root cause by multiplying their respective severity, occurrence, and detection rating [42, 43].

$$\text{RPN} = (\text{Severity}) \times (\text{Occurrence}) \times (\text{Detection}). \quad (1)$$

A root cause of a potential failure with higher RPN indicates it will create higher risk to the network if left unattended. Thus priority will be given to corrective actions recommended for potential failure that is associated with the highest RPN.

A rating of 1 to 10 is typically used to rate the severity of the root causes for the failure on the network performance and the frequentness of occurrence. Fatal impact and inevitable occurrence will be rated with a score of 10 while the lowest score of 1 reflects meagre impact and extremely unlikely occurrence [41–43]. The severity and occurrence rating criteria in FMEA are normally based on various specifications associated with reliability of electronic hardware equipment particularly MTTR (Mean Time to Repair) and MTBF (Mean Time between Failures) [8, 44, 45].

The detection rating scale of 1 to 10 is used to rank the capability or ease of the network to detect the root causes of the potential failures modes identified. A score of 1 will be allotted to network designed to detect with certainty the causes of failures while network without features to detect the causes of failures will be placed on the highest end of the scale.

After determining the RPN, actions will be recommended to reduce the RPN for each root cause. The severity, occurrence, and detection ratings are then reevaluated based on the recommended corrective action to mitigate the failures. The new RPN for each root cause is then calculated and used to analyse the risks presented by the causes of failures and prioritise the corrective actions to be taken.

The method for assigning severity, occurrence, and detection rating scale before and after the recommended mitigation actions for HOWBAN will be discussed in the following subsections.

3.1. Severity Rating Scale. In this paper, a score of 1 to 10 is used to reflect the severity of the failure of a component to the performance of the HOWBAN. The severity is rated based on number and duration of MCs unable to connect

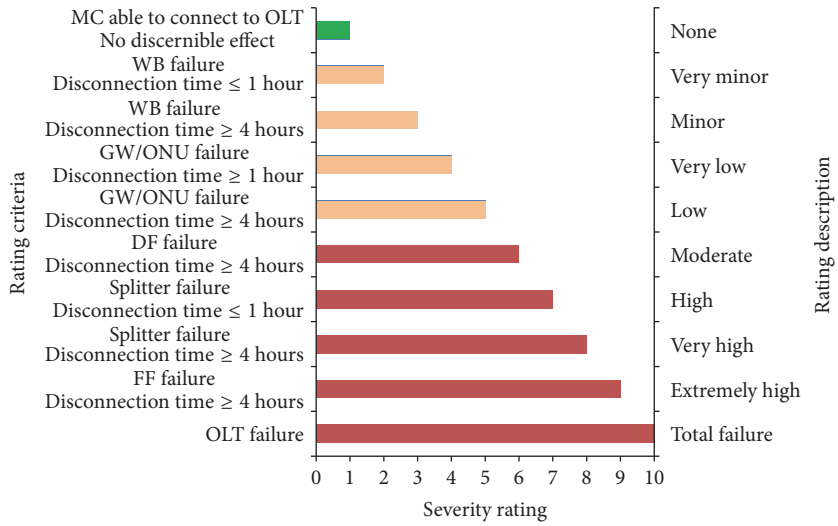

Figure 2: HOWBAN Severity Rating Scale.

to OLT as a result of component failures in a segment of the network. Failure in network component that is closer to OLT will affect more MCs compared to those at the front end and tends to result in higher severity. One of the specifications of a network component that can be used to determine the duration of the failure is Mean Time to Repair (MTTR) which determines how soon the network will recover after experiencing system failures [8, 37, 44]. In an operational system such as the HOWBAN, repair often means replacement of hardware module [44]. Replacement of outside plant and customer premise equipment may need to consider delivery and field work time and is typically rated as between 8 and 24 hours or more [8, 12, 46, 47]. In this paper, the duration of failure is based on MTTR of each of the components. IEEE standard [48] quoted that, for repair or part replacement in the central office, a couple of hours is required. Typical MTTR adopted by telecommunication sector is 4 hours [8, 49]. For outside plant, the MTTR is set at 24 hours [8].

A higher severity rating indicates the increase in the severity of the failure based on the number of MCs affected by the failure in the network components and the time taken to rectify the failure. A rating of 10 is assigned to OLT failure where all MCs are unable to access the Internet. Rating 1 is allocated in condition where all MCs are able to connect to Internet via the OLT.

MC will not be able to connect to OLT when there is failure in WB due to either equipment fault or power outage in the WB/MC segment. WB which failed but required shorter time to repair is rated lower than the WB failure that needs longer time to repair. Thus WB failure with 1-hour disconnection time is given a rating of 2 while that creating 4 hours of disconnection time has a rating of 3.

As GW in the GW/WB segment is typically connected to several WB, when failed, it will affect larger number of MCs and is thus given a higher severity rating compared to WB failure. Gateway failure creating disconnection time of 4 hours is also rated higher with rating of 5 than GW failure

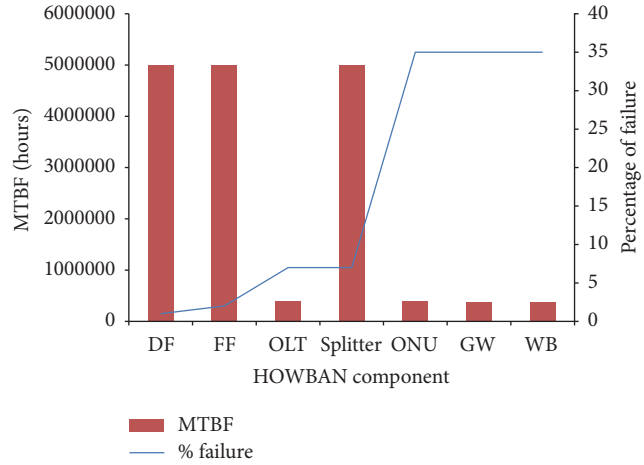

Figure 3: Comparison of MTBF and failure statistics of network component.

that has 1 hour of disconnection time which has a rating of 4. Since the impact of ONU failure in the ONU/GW segment is the same as GW, they are given the same rating. DF failure is accorded higher rating compared to ONU and GW failures as it typically required more time to locate and clear.

Failures in optical splitter and FF are rated higher than DF, ONU, and GW as their failures will have impact on relatively more MC. The severity rating setup is as shown in Figure 2.

The failure percentage of the passive components in the passive optical network is more than 7 times that of active components and Mean Time between Failures (MTBF) is at least 10 times higher [12] as shown in Figure 3 implying that the back end optical network is more resilient than the front end wireless network in terms of equipment failure.

OLT is typically located at central office (CO) and is well protected with redundancy to bring it back into operation within 50 ms [9]; thus its resiliency is considered comparable

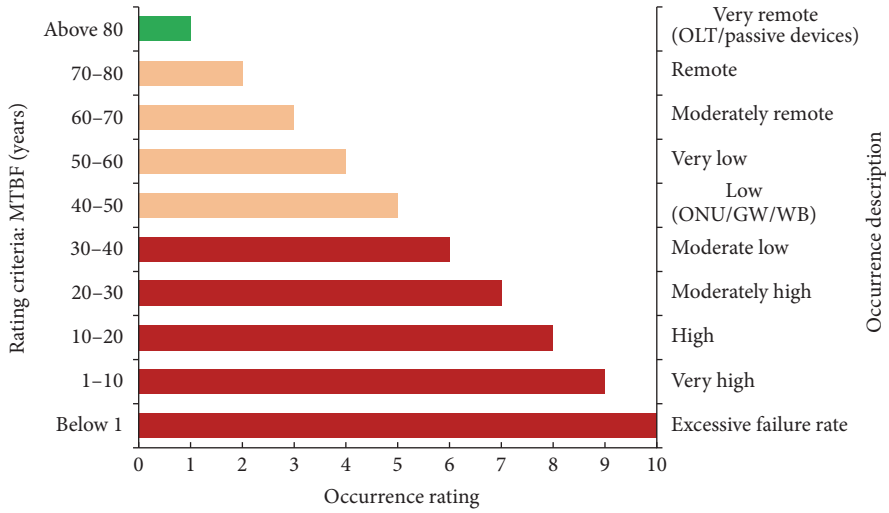

Figure 4: HOWBAN equipment failure occurrence rating scale.

to passive component. It is thus reasonable to focus the evaluation on the faults due to the active components in segments from ONU to WB located at the front end.

The MTTR for all the components from ONU to WB segment are similar since they are all located outdoor; thus their severity rating will just depend on the number of MCs affected. In this paper, we are taking the worst case rating with highest disconnection time for WB, GW, and ONU which are rated 3, 5, and 5 respectively to calculate the RPN.

FMEA required corrective actions to be recommended after the severities of the components on the network failure have been assigned and to rerate the severity factor after performing the corrective actions. In this paper, potential failure due to network component at the front end will be resolved by employing the ubiquitous approach of installing redundant component. Backup battery is recommended for resolving the potential failure due to grid power outages. With single redundant parallel standby equipment installed, the severity factor will be reduced by around half assuming that the equipment will survive to 50% of its rated MTBF [50, 51].

3.2. Occurrence Rating Scale. In severity rating, the same impact on MC is felt whether the failure is due to equipment fault or power outage; thus both are given the same rating. For occurrence rating, the scale for network component fault and power outage in HOWBAN has to be separated as they have difference failure criteria.

The commonly considered specifications for occurrence rating of the HOWBAN network component are Mean Time between Failures (MTBF) [8, 37, 44]. Mean Time between Failure is the average time between failures of a product and is frequently quoted in hours. As MTBF is the inverse of failure rate it can thus be used to indicate the occurrence of the failure in the network component [44, 52, 53]. A relative score range of 1 to 10 is preferred rather than the absolute probability as an absolute probability of 10^{-6} may give the perception that failure occurring is very remote [43]. A fault that is almost certain to occur will be rated with a score of 10. In this paper, the network component occurrence rating scale will rely on MTBF of each of the components. A higher MTBF value is associated with low occurrence.

Table 1: MTBF of network components.

Component	MTBF (hours)	MTBF (years)
OLT	400000	46
FF	5000000	570
Splitter	5000000	570
DF	5000000	570
ONU	400000	46
GW	380000	43
WB	380000	43

Typical MTBF of various components in the HOWBAN listed in Table 1 are quoted from [8, 46] and commercially available devices. ONU, GW, and WB which have MTBF ranging from 380000 hours to 400000 hours or between 40 and 50 years are assigned a rating of 5. OLT is grouped together with the passive devices which have MTBF above 80 years and is assigned a relatively low rating of 1. Although OLT has lower MTBF compared to the passive components in the network, its failure rate is low because it is located at the central office and is typically protected with ample redundancy. This common policy enhances the resiliency of OLT and makes its failure percentage similar to that of passive optical splitter in the network.

The relative occurrence rating of network component in HOWBAN is set up as shown in Figure 4. The rating is consistent with the optical network and outside distribution network failure statistics collected by China Telecommunication Corporation [12] as shown in Figure 3 which showed that the failure percentage of passive devices and OLT are much lower than the front end components.

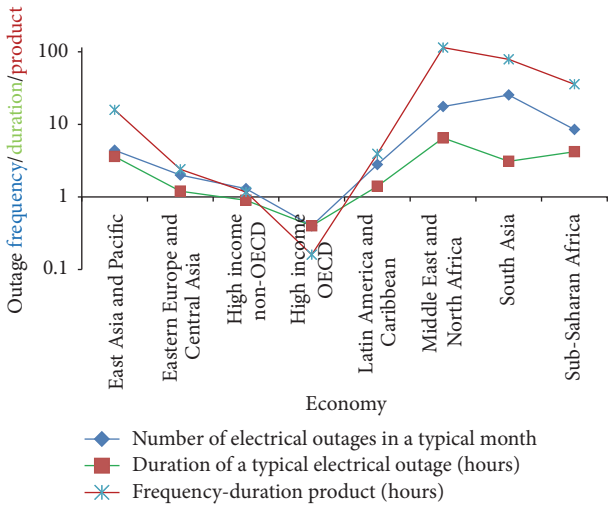

Figure 5: Power outages data.

The occurrence rating for power failure or outage is based on frequency and duration of grid power outage product using the data reported in World Bank enterprise survey as shown in Figure 5 [54]. The highest and lowest frequency and duration of power outage product value derived are 114.4 hours and 0.16 hours, respectively. The highest product values per month are experienced by less developed countries in the Middle East and North Africa while the high income of Organisation for Economic Cooperation and Development (OECD) countries has the lowest product value. Relatively high product value also occurred in South Asia and South Saharan Africa economy compared to the high income countries.

The minimum rating of 1 and maximum rating of 10 are based on the lowest and highest product value derived by multiplying the frequency and average duration of power outages of each economy. The rating scale is as shown in Figure 6. The frequency outage product value above 90 hours is assigned a rating of 10 and a rating of 1 will be accorded to product value below 1 hour.

ITU reported that, as of 2014, the number of broadband users per 100 inhabitants is 83.7 and 21.1 in the developed and less developed countries, respectively [55]. This reflects that there is greater potential for growth and need to expedite the deployment of broadband access to the less developed countries; thus this FMEA evaluation will be based on the less developed economies listed in [54]. As the quality of the grid power in the less developed economies is very poor, the occurrence for failure due to loss of power in HOWBAN is given a rating of 10.

The rating of the occurrence after provision of redundant parallel standby component or backup battery is half that before taking the recommended actions so as to be consistent with assumptions made for the severity rating.

3.3. Detection Rating Scale. Detection of optical network failure typically relied on using OTDR to sense the loss of upstream signal [13]. Faults in HOWBAN can be detected effectively with the availability of improved monitoring and network fault detection strategy such as centralized failure detection system (CFDS) [56] coupled with recently introduced IEEE SIEPON standard [12]. In SIEPON standard, the absence of REPORT/GATE message pair for a duration 50 ms will indicate a link fault. Continuous monitoring of transmission from OLT by ONU shortened the delay in sensing the link fault. The data link from OLT is assumed failed if the valid optical signal is not received within 2 ms after a device is detected and registered in the network. For the wireless mesh network, the multipath nature of the network will enable failed node to be detected and traffic rerouted to alternative route. With the improvement of monitoring and detection standard failures in the optical backend and robustness of the wireless mesh network, failure in HOWBAN can be reliably detected and thus given a rating of 1 in this paper. The detection rating scale is displayed in Figure 7.

4. Results and Discussion

In this paper, the process function identified is to provide connection to Internet via HOWBAN as stated in the first column in Table 2 which is adapted from FMEA evaluation form. The second column merely lists the numbering of the segments at the front end of HOWBAN. The segments that constitute the network will be listed in the third column of Table 2. The network segments may include those in the backhauls and the front end. Total failure of all components in any segment of the HOWBAN will result in total link loss between MC and OLT under the unprotected optical network. However it is extremely unlikely that all components in any segment will completely fail and thus it will be more realistic to evaluate the scenario of partial link loss which is due to partial failure in segments within the network. As explained in Section 3.1, the resiliency of the network component in the backhaul is much higher than those at the front end; thus this evaluation will be focused on the front end. The relevant front end segments, namely, ONU/GW, GW/WB, and WB/MC, are as noted in the third column in Table 2.

For the ONU/GW segment, the potential failure mode identified is GW unable to access the ONU which is connected at its back end as depicted in the first row of the fourth column in the table. The effect of this failure is that traffic from access points (WB) connected to the GW is unable to be forwarded to the OLT thus creating partial link loss in the network as shown in the first row of the fifth column in the table. The severity rating of 5 is assigned to the effect of this failure using the rating scale in Figure 2. The rating is recorded in the first row of the sixth column in Table 2.

Two root causes for this failure mode identified are ONU failure due to equipment faults and loss of power as shown, respectively, in the first and second row of the seventh column in Table 2. The severity, occurrence, and detection rating assigned in Sections 3.1–3.3 for each of the root causes are inserted into the respective row from eighth to tenth column in Table 2.

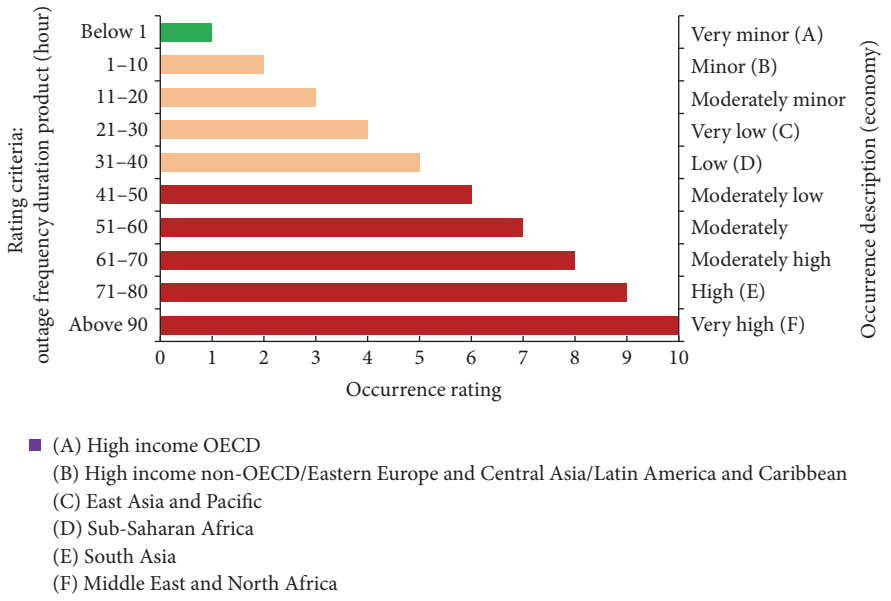

Figure 6: HOWBAN power outages occurrence rating scale.

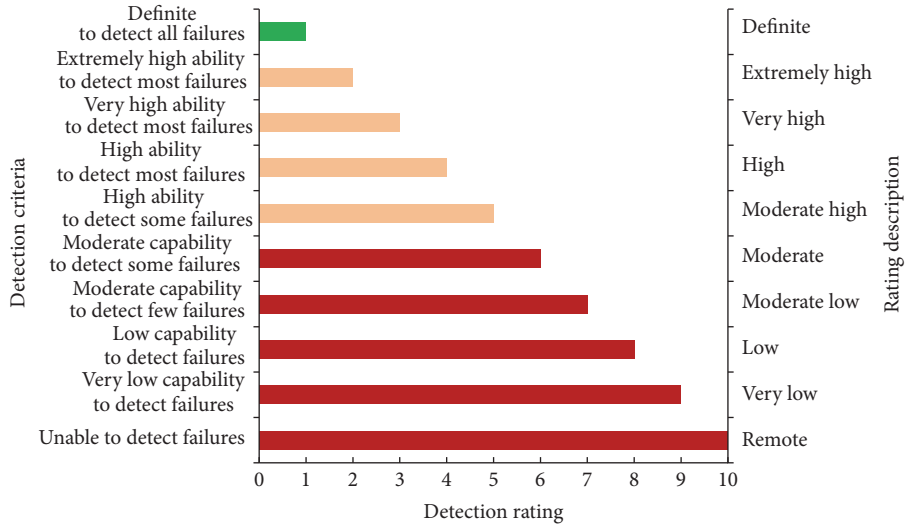

Figure 7: HOWBAN detection rating scale.

The RPN for both of the root causes calculated are then recorded in the first and second row of the eleventh column in Table 2. The recommended actions that can be taken to reduce the severity, occurrence, and detection rating and consequently the RPN for each root cause are entered into the respective row in the twelfth column in the table. Based on the recommended actions to be taken, the severity, occurrence, and detection rating for each of the root causes will be revised. The new ratings are recorded in respective row in the thirteenth to fifteenth column in Table 2. The new RPN are derived and inserted into the respective row in the last column in the table.

The procedure to calculate the RPN is repeated for the potential failure modes for each of the remaining segments identified. The RPN for all the roots causes in all the segments are then used to analyse and identify the potential failure mode and root causes that need priority attention. The full result of the FMEA technique used to analyse the partial link loss scenario in HOWBAN is as shown in Table 2.

The results in Table 2 are plotted in Figure 8. It is evident from the data presented in Figure 8 that the RPN associated with power failures or outages before taking mitigation action, indicated by the cross hatched bar with green boarder, are double that due to equipment failure. It can also be observed that with the provision of redundant equipment and backup power their respective RPN can be reduced by at least 3 times. However, the RPN due to power outages remained higher than that of equipment failure even after mitigation. The high reliability of the communication equipment linked to high MTBF is a factor that equipment failures are

Table 2: FMEA table for partial link loss.

Process function	Number	Network segment	Potential failure mode	Potential effect(s) of failure	Sev	Potential cause(s)/mechanism(s) of failure	Sev	Occ	Det	RPN	Recommended action(s)	Partial redundancy			
												Sev	Occ	Det	RPN
To provide connection to Internet via HOWBAN	1	ONU/GW	GW unable to access ONU	Partial link loss (PLL)	5	ONU failure: ONU lost power	5	10	1	50	Backup battery	3	5	1	15
						ONU failure: equipment failed	5	5	1	25	Redundant ONU	3	2	1	6
	2	GW/WB	WB unable to access partial GW	Partial link loss (PLL)	5	GW failure: GW lost power	5	10	1	50	Backup battery	3	5	1	15
						GW failure: equipment failed	5	5	1	25	Redundant GW	3	2	1	6
	3	WB/MC	MC unable to access partial WB	Partial link loss (PLL)	3	WB failure: WB lost power	3	10	1	30	Backup battery	1	5	1	5
						WB failure: equipment failed	3	5	1	15	Redundant WB	1	2	1	2

Sev: severity; Occ: occurrence; Det: detection.

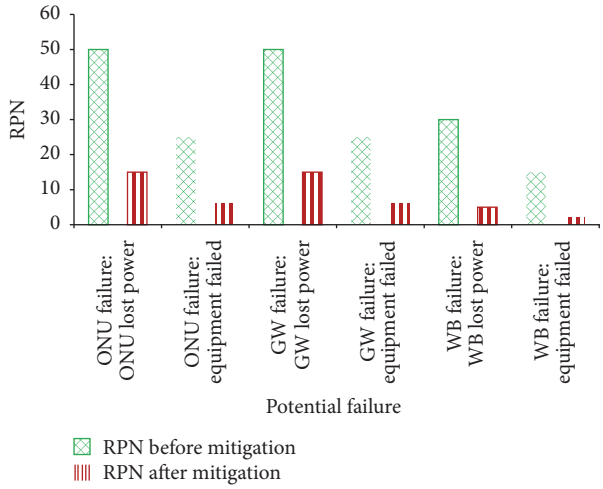

Figure 8: Partial link loss RPN before and after mitigation.

associated with lower RPN compared to power outages in all situations.

This finding is in line with concerns on power outages raised in report on electricity reliability by Pacific Power Benchmarking Report published by Pacific Power Association (PPA) in June 2015 which showed that average SAIDI (System Average Interruption Duration Index) which reflects the average amount of time that customers are interrupted has increased from 592 minutes per customer in 2001 to 5664 minutes per customer in 2012 [57]. Studies conducted by [58] highlighted the deficiency in the reliability of the power grid in India where the typical power outage may be 2 to 8 hours a day in urban area and may exceed 20 hours a day in rural area which reaffirmed the scenario of power outages given in the Enterprise Surveys conducted by the World Bank as shown in Figure 5 [54].

The power outages could be due to unreliable electrical power transmission and distribution system [58, 59] and badly designed substation [60]. Consequently backup power supply is inevitable for the HOWBAN especially for the front end WB which are located at remote areas and less developed countries with unreliable or no grid supply. The backup power system typically consists of combination of standalone power system such as battery and diesel generators [58, 61, 62]. Battery performance and life cycle are sensitive to temperature which has to be kept at around 27°C [58, 63]. The backup battery solution is more expansive for the outside plant due to the harsh temperature environment which required energy for cooling and thus leading to considerable increase in its deployment cost compared to the same solution for the central office [58, 61, 63].

Battery bank either lead acid or lithium type is commonly used to provide the power during power outage. However for extended period of power outages in excess of 8 hours, the battery will be fully drained and need to be recharged. Clearly the battery is able to maintain the HOWBAN operation during outages but the duration is limited. Typical best practice of reserve power in WB in a developed country is quoted as minimum of 4 hours with an objective of 8 hours in [63] while [58] highlighted that backup power is required to support daily outages of 2 to 8 hours in urban area and up to 20 hours in rural areas. To use the battery to support the network power for longer period of time will increase the cost significantly [58, 63–65]. Diesel generator is recommended to support outage period exceeding 8 hours.

The redundant power source must be capable of sustaining communication for MC and network monitoring between the various segments in the network [63]. Backup power system using diesel generator involved not only CAPEX but also OPEX which include cost of the running fuel and maintenance cost [58, 62, 66]. A more detailed study on the cost for the provision of backup power to enhance and optimise the reliability and survivability of HOWBAN is essential for extending the network especially to rural areas and less developed countries which encounter uncertainty in quality of grid power.

5. Conclusions

This paper has highlighted that the grid power failure occurrence is twice that due to equipment failure in all the segments at the front end of HOWBAN thus resulting in the corresponding higher value of RPN. RPN for grid power failure is reduced by deploying backup battery but the value remained higher relative to that of equipment failure due to the low quality of the grid power particularly those in rural areas and less developed economies compared to the high MTBF of the equipment. It is plain that backup power supply is critical for the deployment of HOWBAN especially in rural areas and less developed countries and investigations entailing the optimisation of deployment cost for backup power in HOWBAN are crucial. The studies will assist in hastening the decision for rendering affordable broadband Internet access to empower the deprived community to access the Internet and narrow the digital divide gap which has been identified by ITU as one of the key factors to raise the economy of a nation leading to improvement in the quality of life of people in the world. As wireless communication is also one of the key enablers for Internet of things which is essential for the successful realisation of smart city initiatives there is a need to give impetus to embark on the optimisation study proposed. Failure to address the grid power issue in the rural areas and less developed countries will continue to hinder the progress in the broadband penetration.

Although FMEA is usually deployed before the network is implemented, it must be kept in mind that the variables used in determining the RPN are not constant and may vary under different working environment. It is thus essential to review the FMEA process at regular intervals in line with changes in the technology. Nevertheless FMEA provides an engineering approach to obtain a good overview of the network performance.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] International Telecommunication Union (ITU), The Impact of Broadband on the Economy: Research to Date and Policy Issues, Telecommunication Development Sector, pp. 3–17, April 2012.

[2] S. Sarkar, S. Dixit, and B. Mukherjee, "Hybrid wireless-optical broadband-access network (WOBAN): a review of relevant challenges," *Journal of Lightwave Technology*, vol. 25, no. 11, pp. 3329–3340, 2007.

[3] Z. Zheng, J. Wang, and J. Wang, "A study of network throughput gain in optical-wireless (FiWi) networks subject to peer-to-peer communications," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–6, June 2009.

[4] I. Filippini and M. Cesana, "Topology optimization for hybrid optical/wireless access networks," *Ad Hoc Networks*, vol. 8, no. 6, pp. 614–625, 2010.

[5] N. Ghazisaidi, M. Maier, and C. M. Assi, "Fiber-wireless (FiWi) access networks: a survey," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 160–167, 2009.

[6] S.-C. Lee, S.-W. Tan, E. Wong, K.-L. Lee, and C. Lim, "Survivability evaluation of optimum network node placement in a hybrid fiber-wireless access network," in *Proceedings of the 24th Annual Meeting on IEEE Photonic Society (PHO '11)*, pp. 298–299, IEEE, Arlington, Va, USA, October 2011.

[7] Malaysia, Communication and Multimedia Act 1998: Determination No.1 of 2015: Commission Determination on the mandatory standards for Quality of Service (Public Cellular Service), http://www.skmm.gov.my/skmmgovmy/media/General/pdf/MSQoS-for-Public-Cellular-Service01072015.pdf.

[8] ITU, "Transmission systems and media, digital systems and networks, passive optical network protection considerations," ITU-T G-Series Recommendations—Supplement 51, ITU, Geneva, Switzerland, 2013.

[9] K. Hirose, T. Matsumura, and M. Yamasaki, "Cost-benefit analysis of emergency backup power systems for mission critical applications," in *Proceedings of the 32nd Annual International Telecommunications Energy Conference (INTELEC '10)*, pp. 1–7, Orlando, Fla, USA, June 2010.

[10] Board of Governors of the Federal Reserve System, Consumers, and Mobile Financial Services 2015, March 2015, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

[11] L. Wosinska and J. Chen, "Reliability performance analysis vs. deployment cost of fiber access networks," in *Proceedings of the 7th International Conference on the Optical Internet (COIN '08)*, pp. 1–2, IEEE, Tokyo, Japan, October 2008.

[12] M. Hajduczenia, S. Chengbin, Z. Zhen, H. Elbakoury, S. Kozaki, and M. Matsuoka, "Resilience and service protection for ethernet passive optical networks in SIEPON," *IEEE Communications Magazine*, vol. 50, no. 9, pp. 118–126, 2012.

[13] E. Wong, "Survivable architectures for time and wavelength division multiplexed passive optical networks," *Optics Communications*, vol. 325, pp. 152–159, 2014.

[14] Y. Liu, L. Guo, and X. Wei, "Optimizing backup optical-network-units selection and backup fibers deployment in survivable hybrid wireless-optical broadband access networks," *Journal of Lightwave Technology*, vol. 30, no. 10, pp. 1509–1523, 2012.

[15] B. Kantarci and H. T. Mouftah, "Reliable and fast restoration for a survivable Wireless-Optical Broadband Access Network," in *Proceedings of the 12th International Conference on Transparent Optical Networks (ICTON '10)*, pp. 1–4, July 2010.

[16] T. Feng and L. Ruan, "Design of a survivable hybrid wireless-optical broadband-access network," *Journal of Optical Communications and Networking*, vol. 3, no. 5, Article ID 5759821, pp. 458–464, 2011.

[17] E. S. Son, K. H. Han, J. H. Lee, and Y. C. Chung, "Survivable network architectures for WDM PON," in *Proceedings of the Optical Fiber Communication Conference (OFC/NFOEC '05)*, Optical Society of America, Anaheim, Calif, USA, March 2005.

[18] J. Chen, L. Wosinska, and S. He, "High utilization of wavelengths and simple interconnection between users in a protection scheme for passive optical networks," *IEEE Photonics Technology Letters*, vol. 20, no. 6, pp. 389–391, 2008.

[19] A. M. Chowdhury, M.-F. Huang, H.-C. Chien, G. Ellinas, and G.-K. Chang, "A self-survivable WDM-PON architecture with centralized wavelength monitoring, protection and restoration for both upstream and downstream links," in *Proceedings of the Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference (OFC/NFOEC '08)*, Optical Society of America, February 2008.

[20] S. Sarkar, H. H. Yen, S. Dixit, and B. Mukherjee, "RADAR: risk-and-delay aware routing algorithm in a hybrid wireless-optical broadband access network (WOBAN)," in *Proceedings of the Conference on Optical Fiber Communication and the National Fiber Optic Engineers Conference (OFC/NFOEC '07)*, Optical Society of America, Anaheim, Calif, USA, March 2007.

[21] K. Tanaka and Y. Horiuchi, "1:N OLT redundant protection architecture in ethernet PON system," in *Proceedings of the Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference (OFC/NFOEC '08)*, Optical Society of America, February 2008.

[22] A. Kanungoe, A. Mukhopadhyay, G. Das, R. Banerjee, and R. Das, "A new protection scheme for a combined ring-star based hybrid WDM/TDM PON architecture," *Optical Switching and Networking*, vol. 18, no. 2, pp. 153–168, 2015.

[23] W. T. P'ng, S. Khatun, S. Shaari, and M. K. Abdullah, "A novel protection scheme for Ethernet PON FTTH access network," in *Proceedings of the 13th IEEE International Conference on Networks jointly held with the 7th IEEE Malaysia International Conference on Communications*, vol. 1, pp. 487–490, November 2005.

[24] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[25] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: past, present, and future of programmable networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[26] J. P. Sterbenz, R. Krishnan, R. R. Hain et al., "Survivable mobile wireless networks: issues, challenges, and research directions," in *Proceedings of the 1st ACM Workshop on Wireless Security (WiSE '02)*, pp. 31–40, Atlanta, Ga, USA, September 2002.

[27] S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, "Routing protocols in wireless mesh networks: challenges and design considerations," *Multimedia Tools and Applications*, vol. 29, no. 3, pp. 285–303, 2006.

[28] N. Correia, J. Coimbra, and G. Schütz, "Fault-tolerance planning in multiradio hybrid wireless-optical broadband access networks," *Journal of Optical Communications and Networking*, vol. 1, no. 7, Article ID 5345885, pp. 645–654, 2009.

[29] J. Robinson and E. W. Knightly, "A performance study of deployment factors in wireless mesh networks," in *Proceedings of the IEEE 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 2054–2062, Anchorage, Alaska, USA, May 2007.

[30] D. Benyamina, A. Hafid, M. Gendreau, and J. C. Maureira, "On the design of reliable wireless mesh network infrastructure with QoS constraints," *Computer Networks*, vol. 55, no. 8, pp. 1631–1647, 2011.

[31] G. Narlikar, G. Wilfong, and L. Zhang, "Designing multihop wireless backhaul networks with delay guarantees," *Wireless Networks*, vol. 16, no. 1, pp. 237–254, 2010.

[32] S. Sarkar, H.-H. Yen, S. Dixit, and B. Mukherjee, "A novel delay-aware routing algorithm (DARA) for a hybrid wireless-optical broadband access network (WOBAN)," *IEEE Network*, vol. 22, no. 3, pp. 20–28, 2008.

[33] M. Kiese, E. Georgieva, D. Schupke, B. Mukherjee, and J. Eberspächer, "Availability evaluation of hybrid wireless optical broadband access networks," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–6, Dresden, Germany, June 2009.

[34] A. Goel and R. J. Graves, "Using failure mode effect analysis to increase electronic systems reliability," in *Proceedings of the 30th International Spring Seminar on Electronics Technology*, pp. 128–133, IEEE, May 2007.

[35] M. G. Pecht and F. R. Nash, "Predicting the reliability of electronic equipment," *Proceedings of the IEEE*, vol. 82, no. 7, pp. 992–1004, 1994.

[36] C. J. Creveling, "Increasing the reliability of electronic equipment by the use of redundant circuits," *Proceedings of the IRE*, vol. 44, no. 4, pp. 509–515, 1956.

[37] M. Krasich, "How to estimate and use MTTF/MTBF would the real MTBF please stand up?" in *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS '09)*, pp. 353–359, IEEE, Fort Worth, Tex, USA, January 2009.

[38] R. Bono, R. Alexander, A. Dorman, Y.-J. Kim, and J. Reisdorf, "Analyzing reliability—a simple yet rigorous approach," *IEEE Transactions on Industry Applications*, vol. 40, no. 4, pp. 950–957, 2004.

[39] IEEE, "IEEE guide for selecting and using reliability predictions based on IEEE 1413," IEEE Std. 1413.1-2002, 2003.

[40] Department of the Army, Washington DC, Failure Modes, Effects and Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 2006, https://www.wbdg.org/ccb/ARMYCOE/COETM/tm_5_698_4.pdf.

[41] ReliaSoft—Xfmea Report Sample—Design FMEA, http://www.reliasoft.com/pubs/xfmea_dfmea.pdf.

[42] Sydney Water, *Failure Mode Effects and Criticality Analysis (FMECA)*, 2010, http://www.sydneywater.com.au/web/groups/publicwebcontent/documents/document/zgrf/mdq2/~edisp/dd_046414.pdf.

[43] Warwick Manufacturing Group, 2007—Failure Modes, Effects and Criticality Analysis, http://www2.warwick.ac.uk/fac/sci/wmg/ftmsc/modules/modulelist/peuss/slides/section_12a_fmeca_notes.pdf.

[44] S. Stanley and IMC Networks (USA), MTBF, MTTR, MTTF & FIT: Explanation of Terms, http://www.bb-elec.com/Learning-Center/All-White-Papers/Fiber/MTBF,-MTTR,-MTTF,-FIT-Explanation-of-Terms.aspx.

[45] IEEE Standard, "IEEE standard framework for reliability prediction of hardware," IEEE Std 1413-2010, Revision of IEEE Std 1413-1998, 2010.

[46] CORDIS, "EU—Technical Assessment and Comparison of Next-Generation Optical Access System Concepts," 2011, http://cordis.europa.eu/docs/projects/cnect/5/249025/ 080 /deliverables /001-OASED421 WP4UEssex 31Oct2011 V10.pdf.

[47] J. Chen, L. Wosinska, C. M. MacHuca, and M. Jaeger, "Cost vs. reliability performance study of fiber access network architectures," *IEEE Communications Magazine*, vol. 48, no. 2, pp. 56–65, 2010.

[48] IEEE P1904.1™/D2.5 Draft Standard for Service Interoperability in Ethernet Passive Optical Networks, June 2012.

[49] China Telecom Business Characteristics, http://www.chinatelecomglobal.com/subsite/indonesia.html.

[50] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems—Concepts and Techniques*, Springer, New York, NY, USA, 2nd edition, 1992.

[51] S. Speaks, Vicor Reliability Engineering, Reliability and MTBF Overview, http://www.vicorpower.com/documents/quality/Rel_MTBF.pdf.

[52] J. G. McLeish, "Enhancing MIL-HDBK-217 reliability predictions with physics of failure methods," in *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS '10)*, pp. 1–6, January 2010.

[53] ITEM Software, "Reliability Prediction Basics," 2007, http://www.reliabilityeducation.com/ReliabilityPredictionBasics.pdf.

[54] Data on Infrastructure World Bank Enterprise Survey of Business Managers World Bank Group, http://www.enterprisesurveys.org/data/exploretopics/infrastructure.

[55] *Trends in Telecommunication Reform 2015*, ITU, Geneva, Switzerland, 2015, http://www.itu.int/en/publications/Documents/Trends2015-short-version_pass-e374681.pdf.

[56] M. S. Ab-Rahman, B. C. Ng, and K. Jumari, "Detecting faulty fiber with centralized failure detection system (CFDS) in fiber-to-the-home (FTTH) access network," *Optica Applicata*, vol. 39, no. 2, pp. 241–250, 2009.

[57] Pacific Power Association (PPA), Pacific Power Benchmarking Report, Fiscal Year 2012, Jun 2015, http://www.ppa.org.fj/wp-content/uploads/2015/08/PPA-Power-Benchmarking-Final-Report-2012-Fiscal-Year.pdf.

[58] A. Jhunjhunwala, B. Ramamurthi, S. Narayanamurthy, J. Rangarajan, and S. Rahj, Powering Cellular Base Stations: A Quantitative analysis of energy options, Telecom Center of Excellence (RiTCOE), Indian Institute of Technology, Madras, https://natgrp.files.wordpress.com/2012/10/powering-cellular-base-stations-a-quantitative-analysis-of-energy-options-prof-ashok-jhunjhunwala-ritcoe-iit-madras.pdf.

[59] M. Al-Muhaini, G. T. Heydt, and A. Huynh, "The reliability of power distribution systems as calculated using system theoretic concepts," in *Proceedings of the IEEE Power and Energy Society General Meeting*, pp. 1–8, IEEE, Minneapolis, Minn, USA, July 2010.

[60] X. Xu, B. Lam, R. Austria et al., "Assessing the impact of substation-related outages on the network reliability," in *Proceedings of the IEEE International Conference on Power System Technology (PowerCon '02)*, vol. 2, pp. 844–848, Kunming, China, October 2002.

[61] T. H. Sloane and D. Olps, "Telecom engine generators for backup powering solutions," in *Proceedings of the AMTC*, Alpha Technologies Inc, July 2000.

[62] S. A. Chowdhury and S. Aziz, "Solar-diesel hybrid energy model for Base Transceiver Station (BTS) of mobile phone operators," in *Proceedings of the 2nd International Conference on the Developments in Renewable Energy Technology (ICDRET '12)*, pp. 1–6, January 2012.

[63] California Public Utilities Commission, *Reliability Standards for Telecommunications Emergency Backup Power Systems and Emergency Notification Systems California Public Utilities Commission, Final Analysis Report*, California Public Utilities Commission, 2008.

[64] S. Moury, M. Nazim Khandoker, and S. M. Haider, "Feasibility study of solar PV arrays in grid connected cellular BTS sites," in *Proceedings of the International Conference on Advances in Power Conversion and Energy Technologies (APCET '12)*, pp. 1–5, IEEE, Andhra Pradesh, India, August 2012.

[65] Sira Pakistan—Solar RBS, http://www.sira.net/Brochure/bts.pdf.

[66] P. Nema, R. K. Nema, and S. Rangnekar, "PV-solar/wind hybrid energy system for GSM/CDMA type mobile telephony base station," *International Journal of Energy and Environment*, vol. 1, no. 2, pp. 359–366, 2010.