Addressing Service Availability parameters in Service Providers using Technology as a Complex System

Tarek Heggi[1], Maryam Hazman[2], Fathy Amer[3], Reem S. Abdallah[4]

[1,2]Central Lab. for Agricultural Expert Systems, Agricultural Research Center, Egypt
[3]Faculty of Computers and Information, Cairo University, Egypt
[4]Faculty of Engineering, Cairo University, Egypt

ABSTRACT

Service providers relay on different technologies such as Broadband and FTTx to provide their services and customer satisfaction is an essential objective. Reliability represents an essential requirement for the customer. Time and performance are components of reliability. There are a lot of parameters that are taken into consideration to achieve performance and consequently customer satisfaction. To guarantee Operation and Service Level Agreement (OLA and SLA) among the different entities in the Service Provider Organization and between the customer and service provider, the service provider should state the parameters that have an impact on achieving reliability of the system. This research paper conducted a risk assessment using the Preliminary Risk Assessment to state and prioritize the parameters that have an impact on achieving the high reliability of the system. The results from this research indicate that the percentage of the risks are 26.7 % in the power subsystem, 23.3% in the backbone subsystem, 16.7 % in the access subsystem, 10 % in the optical distribution network, 10 % in the application server, 3.3 % in the lack of materials, 3.3 % in the security safety subsystem, and 3.3 % in the security attacking subsystem. After assessing the risks in the service provider system, it discusses the required controls to mitigate or eliminate these risks.

Index Terms: Service Level Agreement, Risk Assessment, Preliminary Risk Assessment.

I. INTRODUCTION

The emerging of new applications that require high bandwidth has led the trend for using new network architectures such as FTTx system. FTTx System uses either P2P or GPON architecture depending on the target users. Cost Analysis mode that is proposed by [1] compare between GPON and P2P which illustrates that the P2P cost is on average 15% greater than GPON and this percent is varying based on two parameters which are: take-up rate and geographical area [2]. Some other case studies like [3] stated that the difference in Capital cost between GPON and Active Ethernet (AE) is 5 % whereas, the Operation cost in GPON is lower than AE by 5 to 58% based on to the take-rates. There are a lot of comparative analyses for evaluating these two architectures but it is beyond the scope of this research. This research will address and prioritize the organization parameters that are concerned with the achieving of service availability.

The essential metrics for evaluating the network performance include: availability, delivery, latency, and bandwidth [4]. Availability represent the continuity of the service. Reliability means performance over time, or in a formal definition per [5] “the probability of components, parts, and systems to perform their required functions for a desired period, without failure, in specified environments with desired confidence”. Another important definition for reliability is “Quality over time” [6]. Thus, reliability includesthe availability and functionality of the system. The functional of the system is represented in network performance and operation.

II. METHODOLOGY

This work has been adapted the following steps to conduct the risk assessment to running systems:
1- Selecting the suitable technique to be applied
2- Define system in terms of its components and functions
3- Identify hazards of the system
4- Identify parameters of risks evaluation and decisions
5- Analyzing and mapping risk scenarios
6- Identify controls

III. SELECTION CRITERIA FOR RISK ASSESSMENT TECHNIQUE

There are too many approaches to implement the risk assessment, this study used the preliminary risk assessment (PRA) [7] analysis due to the following reasons:

- Suitable to be applied on operation phase [8-9]
- It provides both qualitative and semi quantitative analyses [10]
- It is a systemic approach which supports complex systems which composed of several actors and relationships that can include elements other than work processes such as environment, and staff [11-13].
- Usability, its implementation process is well documented.
- Popularity, it has been used in many applications

IV. RISK MANAGEMENT OVERVIEW

Figure 1 indicates the methodology that will be applied which follow the systemic approach as in [13, 14].

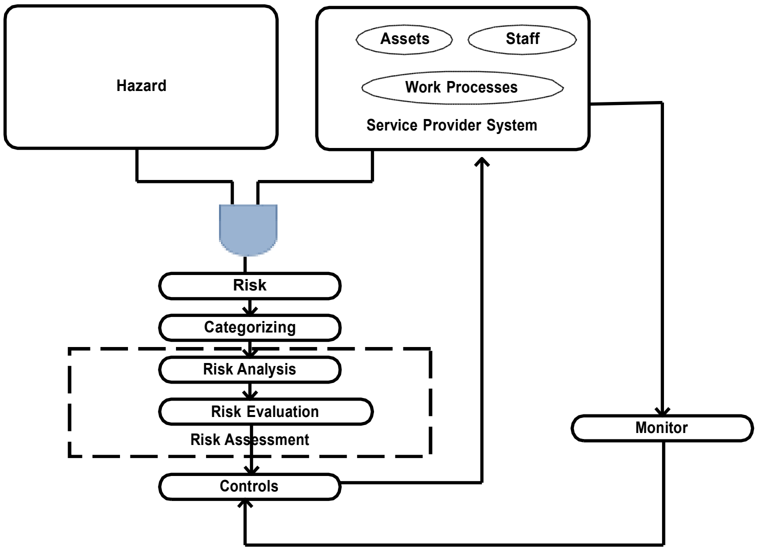

Figure 1. Application of PRA for Risk Management

V. OVERALL SYSTEM RELIABILITY

The reliability of the system reliability is measured using the quality of its provided services and the up time of the services. There are three terms that are used to calculate the total service downtime and the system availability percent which are: repair, means the fault caused the node failure and it should be repaired, one of the method of

repairing is the replacement [15], recovery is a stage after repair which mean to system complete its procedures to be started/loaded then restore after the completion of recovery, the system is considered restored [15].
Availability have different perspective from different vendors, [16] indicates three significant components: device, network, and operational. On the level of device component, it is affected by parameters such as redundancy, hot swapping, modularity, and in service software upgrade [16]. On the level of network, it is affected by parameters such as access control, redundancy in its devices, and Quality of service [16]. on the level of operations, it is affected by parameters such as: open standards, and automate operational tasks [16].

Availability is represented by the percentage of the uptime that the system is running, to achieve the high availability means that this percentage should be either 99.999 % or 99.9999 % which are equivalent to the downtime shouldn't exceed 5 minutes, and 30 seconds respectively in a year [17]. During our calculating the availability, basic differences are needed to be explained before going into implementation as they will assist us in selecting the appropriate controls that can increase the system availability.
There are multiple methods to calculate the availability [18] [19] [20], one of them is the probability of the system is down if both Node 1 and Node 2 are down. The system availability is assumed to be "A", and the probability of failure is "F".
We will consider three scenarios, Figure 2 and Figure 3 indicate the active/active system in which the availability is calculated as follows:

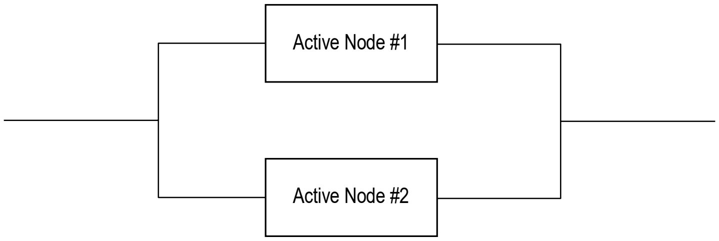

Figure 2. Two Active/Active Nodes System

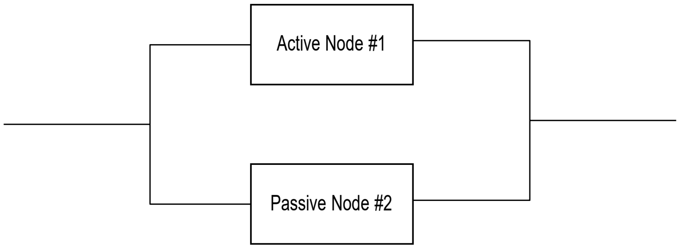

Figure 3. Two Active/Passive Nodes System

For Active/Active and Active/Passive System, assuming that the availability of each node is "a", and the probability of failure on Node 1 = F

$F = 1 - a$, for node 1 and node 2
$A = 1 – (1-a)\ (1-a)$
$= 1 – (1-a)^2 = 1 – (1 - 2a + a^2)$
$= 1 - 1 + 2a - a^2$
$= a\ (2-a)$ equation (1)

The difference between Active/Active and Active/Passive systems include the switch over time in Active/Passive, the complexity of system in Active/Active system and the fully loaded time in the Active/Active system.
For Serial Components in Figure 4 represent a system that consists serial nodes or components.

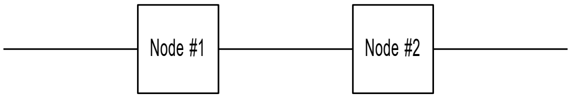

Figure 4. Serial Nodes System

Assuming that Node 1 has availability “a_1” and Node 2 has availability “a_2” then

$$A = a_{1.}a_2$$

For calculating Availability in individual components [20] [21] [22] [23] [24], mean time between failure (MTBF) for reliability and mean time to repair (MTTR). From MTBF and MTTR are known, the availability of the component can be calculated using the following formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$ [25]

Evaluation of the system reliability relies on the contribution of its components and the design of these components, parallel components provide higher reliability than serial components, which means that changes in the design can have a great significant improvement in the reliability [26]. availability can be calculated using the following formula A = u/ (u + d) where u is the uptime, d is the downtime [26].

There are many reliability models that can be used for the system such as Petr Net, Markov, and Monte Carlo simulation [27].

VI. Preliminary Risk Assessment (PRA) Model

The risk of an event can be defined as an abstract concept that consider past, present, and future [28]. According to this definition, the parameters that are considered to calculate the risk of the event are defined. These parameters are the probability of occurrence of the event and its severity [28]. The decision for classifying the risk and putting them into categories depends on the value of the product of the two valued for the probability and the severity [28]. During the defining system in terms of its components and its processes. An example for categories of risk as indicated in Table 1. Figure 5 explains how the risk is created from the interaction between the components of the system and the hazards though a root cause or initiator [30].

Table 1. Risk Categories

		Severity				
		1	2	3	4	5
Probability	5	1	🟨	🟥	🟥	3
	4	1	🟨	🟨	🟥	3
	3	1	🟩	🟨	🟥	3
	2	1	🟩	🟨	🟨	3
	1	1	🟩	🟩	🟨	2

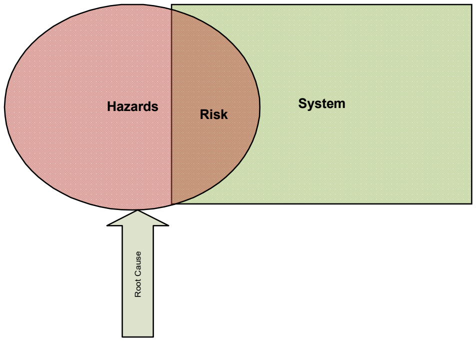

Figure 5. Risk Structure

VII. Implementation

This research will identify the parameters that have impact of reliability in the network system which is responsible for providing services form the service provider to the customers. The FTTH system is considered as a complex system because this system constitutes from different functional blocks that act different activities and all blocks should be operated to be able to provide the services to customers. This research will apply risk management approach to identify these parameters that impact the provisioning of QoS and guarantee the SLA. Risk is identified as the combination of the probability of occurrence of a hazard generating harm in each scenario and the severity of that harm, Hazard is a potential source of harm, the likelihood is the probability of occurrence of that harm [30]. Also, Risk can be identified as effect of uncertainty on objectives” [31]. The third definition of risk is “the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence" [32]. To determine the risk identification for a system, there are is no standard risk classification that can be implemented to any type of organization as mentioned by ISO 31000 for Enterprise Risk Management.

VIII. Service Provider Configuration Scenario

In FTTH scenario, this system that consist of two functional blocks, Access and Core and they represent the main block that must be exist to provide the service to the residents. Figure 6 illustrates the system block diagram.

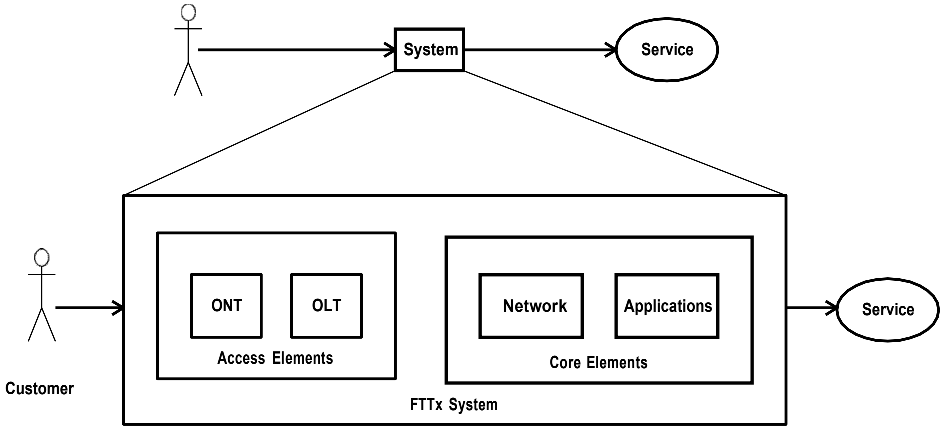

Figure 6. FTTH System Block Diagram

This system consists of elements for access, core, and applications. Access elements include ONT, OLT, and PON. Figure 7 indicated the elements of the access network. OLT represents the element that aggregates all termination that comes from splitters. ONT represents that equipment that is installed in customer side and connects the customer devices such as IPTV STB, access points, phones, and computers. Passive Optical Network (PON) represents the fiber cabling system between data center and customer units.

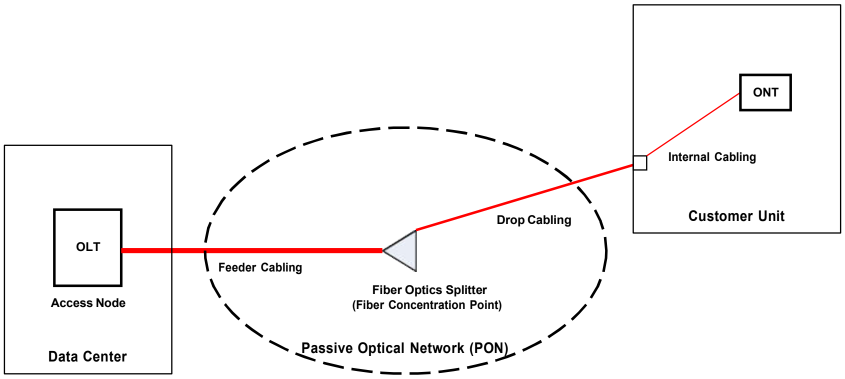

Figure 7. Structure of Access Network

The Access system is considered as a complex system because it consists of multiple subsystems and interventions from different actors. Operation deficiency in any component of the system has an impact on the overall performance and availability of the service. The elements definition per [33], Access Node represents the OLT, Feeder Cabling represents fiber cables from OLT to fiber optics splitter. Fiber optics splitter is the fiber concentration point (FCP). The internal cabling system represented the indoor fiber cable. To maintain the proper operation from dB power perspective, during operation a verification process to ensure the received power meets the vendor thresholds to ONT element, i.e., received power to ONT doesn't be less than-28 dB or more than -28 dB. As per [33], the following equation can be used for this verification Loss = $L_{cable} + L_{splice} + L_{connector}$, this verification is use during design phase and in operation phase, the troubleshooting will include these parameters. Also, it worth to mention that FTTH network lifetime could be 30 years or more [33].

IX. TECHNIQUES TO IDENTIFY UNCERTAINTIES

This study will rely on historical data for previous periods that will be collected through email messages, meetings with different levels of staff, cases with support companies, and customer feedback reports.

Hazard categories can be classified into the following groups as shown in table 2 the below categorization is based on actual status in addition to the assistance of terms and categories in [16]:

Table 2. Preliminary Risk Assessment for FTTH Service Provider Hazard Mapping

17	65	3
General Hazards	**Specific Hazards**	**Source of Hazard**
Power Outage	UPS	Battery
		Rectifier
		Inverter
		Static bypass switch
	Generator	Fuel
		Battery
		Sensors
		Filters
		Oil
	ATS Panel	Battery
		Contactors/Circuit Breakers
		connections
	Power Distribution Panel	Contactors/Circuit Breakers
		connections
		location
	Main Power Source	Egyptian Electricity Holding company (EEHC)
		Contactors/Circuit Breakers/Fuse
		connections
Air Conditioner Failure	Air Conditioner	cooling efficiency
Partially failure in Optical Distribution Network (ODN)	Hardware	splitter
		Fiber Feeder Cable
		Outdoor Fiber Drop Cable
		Fiber Patch Cord
Backbone System Failure		Power supply
		FAN
		backplane
		switching fabric
		Line Card
		Physical Fiber Ports
	Software	IOS/Firmware
		unsupported Version
		upgrading
	Configuration	Applying new features
		Modifying existing features
	Human Error	uncontrolled changes or mistakes during configuration
Access System Failure	Hardware	Rectifier
		FAN
		backplane

		switching fabric
		Line Card
		Physical Fiber Ports
	Software	Firmware
		unsupported Version
		upgrading
	Configuration	Applying new or modifying existing features
	Human Error	uncontrolled changes or inadvertently mistakes during configuration
Application Server Failure	Hardware	Power Supply
		HDD
		Board/CPU
	Operating System	Network Security
	Human Error	uncontrolled changes or inadvertent mistakes during configuration
Lack of Material and Tools	Dysfunction	Shortage of office supplies (paper, files, envelops)
		Disturbance of cars distribution movement
		Failure of computers
		Testing Tools
		Failure of office machines (photocopier, plotter, printer, Fax)
Safety System Failure	Dysfunction of Safety system	Fire Fighting
		Fire Alarm
Attacking System Security	Dysfunction of Physical Security	Surveillance
		Access Control
		Intrusion Detection
	Dysfunction of Network Security	Antivirus
		Firewall
Documentation		Procedures
		Technical Documentation
		External Maintenance Procedures
Customer		Out of scope requirements
		Irrelevant time
Staff		Number of Staff is not sufficient for specific Tasks
		No defined Career path
Supportive entities	Purchasing	Delay in completing procedures
	External Maintenance	Checklist for maintenance procedures is not sufficient
		The company is not committed to response time

The severity impact, the probability, and category of risks are configured as show in Table 3, Table 4, and Table 5.

Table 3: Severity of System Risks

Level	**Index**	**Consequences**
Insignificant	10	No impact on system performance
	11	Its influence is service interruption on limited number of customers due to reasons related to customer
	12	Delay in troubleshooting due to customer issues such as irrelevant time
Low	20	Inferior performance
	21	the impact is on one customer due to the normal operation such as upgrade process of his/her device

		Delay in troubleshooting due to internal issues such as the testing tools are not exist or not working
Major	30	Serious alarm of the performance
	31	its impact is on a group of customers due to distribution cable cut or failure in Physical Fiber interface for one time per 6 months for less than 12 hours
	32	Intermittent Service Failure due to over utilization in core/access/server equipment or cooling efficiency
Critical	40	Service Down
	41	Power/Cooling Failure for more than one time per 3 months for more than 12 hours
	42	Network (Core/Access/Server) Failure for more than one time per 3 months for more than 12 hours

Table 4: Probability of Risks

V1	Rarely occurred	1	Less than one time per T1	
T1				1 year
V2	Possible	2	Less than one time per T2	
T2				6 Months
V3	Major	3	Less than one time per T3	
T3				3 Months
V4	Critical	4	Greater than one time per T3	
P4	High	4		

Table 5: Risk Categories

Risk Category	Description	Index	Type of decision or action
C1	Acceptable	1	No action is required to be taken
C2	Tolerable	2	Risk is within accepted limits but need monitoring
C3	Inadmissible	3	Risk is need control measures
C4	Inacceptable	4	Risk refused

X. Results

The analysis of the APR indicates the risk categories which are indicated in table 6. The hazard situation and their possible risks which generate from the possibility of interaction among the system elements and the hazard.

Table 6. Risk Categories

General Hazard	Abbreviation	Hazard Situation (HS)	Risk Scenario (RS)
Power Outage	PWO	5	8
Air Conditioner Failure	ACF	1	1
Partially failure in Optical Distribution Network (ODN)	ODNF	1	3
Backbone System Failure	BSF	2	7
Access System Failure	ASF	3	5
Application Server Failure	APSF	3	3
Lack of Material and Tools	LMT	1	1
Safety System Failure	SSF	1	1
Attacking System Security	ATT	0	1
Documentation	DOC	0	0
Customer	CUS	0	0

Staff	STF	0	0
Supportive entities	SUPP	0	0

The results in table 6 are represented in Figure 8, which indicated that the risks with higher probability in order are: power outage (PWO), Backbone System Failure (BSF), Access System Failure (ASF), Partially failure in Optical Distribution Network (ODNF), and Application Server Failure (APSF), Air Conditioner Failure (ACF), and Lack of Material and Tools (LMT), and Safety System Failure (SSF), and Attacking System Security (ASS).

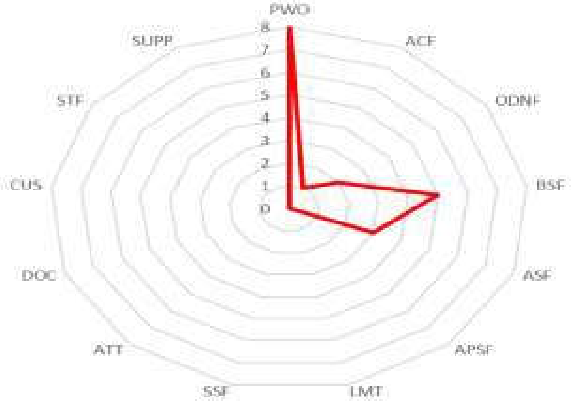

Figure 8. Risk Analysis for Service Provider System

Figure 9 indicated percent of the source of hazards as follows: 26.7 % in the power subsystem, 23.3% in the backbone subsystem, 16.7 % in the access subsystem, 10 % in the optical distribution network, 10 % in the application server, 3.3 % in the lack of materials, 3.3 % in the security safety subsystem, and 3.3 % in all the security attacking subsystem,

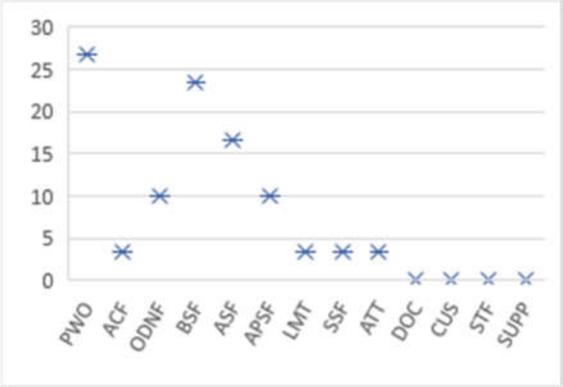

Figure 9. Percentage of System Risks by Source of Hazards

XI. DISCUSSION FOR CONTROLS

Power outage was the highest source of risks, the main parts of UPS element in power system are: Inverter, rectifier battery, and static bypass switch. studies [35] stated that inverter is the most important part that impact on reliability. therefore, we proposed the following controls to reduce the severity of this source by putting batteries into parallel groups instead of one group and each group should maintain the UPS running for 10 minutes on actual load, recording the manufacturing date of the battery, the installation date, and periodically verify the efficiency of the battery quality through the checklist that is executed by the maintenance company. These controls will increase the availability from 99.9 % (This value is for a well-known brand name) for a single UPS system and it translated to 9 hours of outage per year. Per equation (1), the implementation of this control will cause the availability to be:
A = a (2-a) = 0.999(2-0.999) = 99.9999 % which reduces the outage time to 3 secs.

Backbone system was the second source of risks, if for one major element in the backbone system, its component is indicated in the Figure 10. This element is assumed to be 99.974 %. The proposed controls were Ensuring the proper configuration for the two power supplies, monitoring fan status either through NMS or manually, ensuring reliability of the current backplane as it considered as a passive element, the response time in the support contract, evaluate other network designs.

Regarding the access system failure. It was the third of risks, if the OLT element has an availability of 99.943 %. The following are the controls: following up a configuration change procedures, having a test lab to verify the results of any changes, having a testing checklist to verify any new changes, continues monitoring for utilization on Cards, having redundant line card, having fiber spare cables, the number of additional cables needs more investigation, the generated error is listed in the release note of the new version or approved by the vendor, periodical checking for the new firmware versions and the list of fixed bugs, replicating the error cases, following up the procedures of escalating with the vendor, and Verification procedures for any changes in configuration.

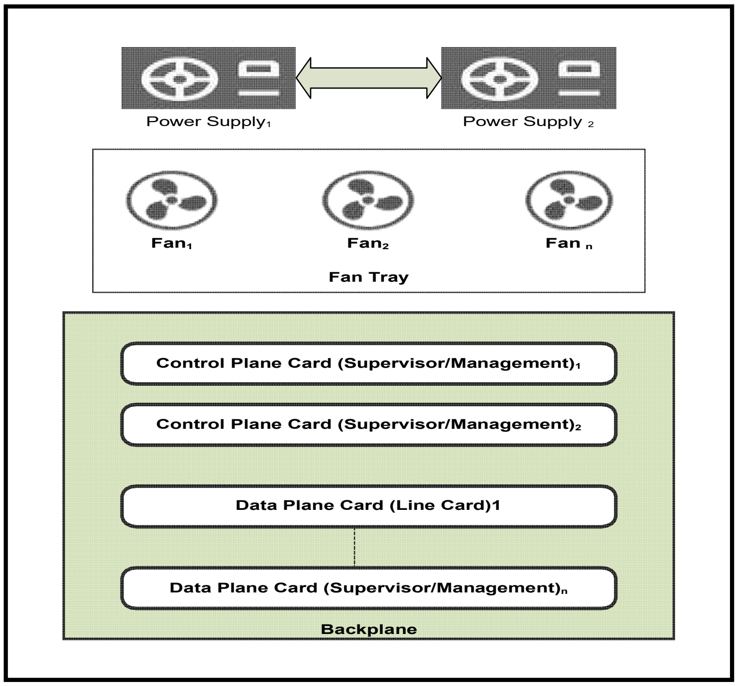
Power Supply₁
Power Supply ₂
Fan₁
Fan₂
Fan ₙ
Fan Tray
Control Plane Card (Supervisor/Management)₁
Control Plane Card (Supervisor/Management)₂
Data Plane Card (Line Card)1
Data Plane Card (Supervisor/Management)ₙ
Backplane

Figure 10. Backbone Element

Partially failure in Optical Distribution Network (ODNF), it has a 10 % of risks. The controls that are proposed are: availing as possible protection for the paths of fiber cables, having sufficient spare parts, and having trained staff or maintenance contract, ensuring the proper installation in protected path for outdoor cables, and implementing type B protection for business customers.
Calculating The availability of the entire system needs to have the availability of each subsystem the get the product of the all these subsystems to get the overall as follows:

$T = ?^{n}_{a} A,$

$T = A_1 \text{ x } A_2 \text{ x } A_3 \text{ x } A_4 \text{ x } A_5 \text{ x } A_6$

Where,

- n equals the number of the subsystem
- A_1 = Availability of the power subsystem
- A_2 = Availability of the backbone subsystem
- A_3 = Availability of the access subsystem
- A_4 = Availability of the optical distribution network subsystem
- A_5 = Availability of the processes
- A_6 = Availability of human factor

CONCLUSION

Not only assets that have an impact on the availability of complex system but other elements as the lack of materials, the security safety subsystem, and the security attacking subsystem have a considered a total of 9.9 % of risks in addition to the human error. if we consider that power outage represents 100% this value of these three sources will be 37.1 % without adding the human factor. Supportive work processes are another source of hazards. This research needs cost analysis for the required controls to compromise among the cost of these controls. Also, the duration time of failure should be considered as a variable because the longtime of failure is considered as a high severity source of hazards even it is caused for limited number of customer and it expose the service provider for a bad image and have a bad impact on customer experience.

REFERENCES

[1]. Mason, Analyses. "The costs of deploying fibre-based next-generation broadband infrastructure." Final report for the Broadband Stakeholder Group 8 (2008): 12726-371.

[2]. Jay, Stephan, Karl-Heinz Neumann, and Thomas Plückebaum. "The cost of nationwide fibre access in Germany." Communications & Strategies 85 (2012): 169-188.

[3]. Kulkarni, Samrat, et al. "FTTH network economics: key parameters impacting technology decisions." Telecommunications Network Strategy and Planning Symposium, 2008. Networks 2008. The 13th International. IEEE, 2008.

[4]. Lee, Hyo-Jin, et al. "QoS parameters to network performance metrics mapping for SLA monitoring." KNOM Rev 5.2 (2002).

[5]. Critchley, Terry. High Availability IT Services. CRC Press, 2014.

[6]. Tixier, Jerome, et al. "Review of 62 risk analysis methodologies of industrial plants." Journal of Loss Prevention in the process industries 15.4 (2002): 291-303.

[7]. Desroches, Alain. "Notion de risque et approche de la maîtrise des risques.", 2011

[8]. de Andrades, Silvana Alves, André Nagalli, and Ronaldo Luis dos Santos Izzo. "Preliminary Risk Analysis in the Operation of a Sanitary Landfill." Electron. J. Geotech. Eng 19 (2014): 3167-3177.

[9]. Perdaman Industries, GHD, "http://www.perdaman.com.au/media/7503/section%206%20-%20preliminary%20risk%20assessment.pdf" visited on 21 February 2017.

[10]. Tixier, Jerome, et al. "Review of 62 risk analysis methodologies of industrial plants." Journal of Loss Prevention in the process industries 15.4 (2002): 291-303.

[11]. SILVA, Meuris Gurgel Carlos da, and Samira Maria Leão de CARVALHO. "Preliminary risk analysis applied to the handling of health-care waste." (2002).

[12]. Chorowski, M., Ph Lebrun, and G. Riddone. "Preliminary risk analysis of the LHC cryogenic system." Advances in cryogenic engineering. Springer US, 2000. 1309-1316.

[13]. Network Infrastructure Committee. "FTTH Infrastructure Components and Deployment Methods, 2007."

[14]. Dumbravă, Vasile, and Vlăduț-Severian Iacob. "Using Probability–Impact Matrix in Analysis and Risk Assessment Projects." Descrierea CIP/Description of CIP–Biblioteca Naționalăa României Conferința InternaționalăEducațieși Creativitate pentru o Societate Bazatăpe Cunoaștere–ŞTIINȚE ECONOMICE (2013): 42.

[15]. The Availability Digest, Calculating Availability – The Three Rs,"www.availabilitydigest.com/private/0103/calculating_availability_three_rs.pdf",Visited on 14, January 2017

[16]. Dell Inc., "Datacenter Class Reliability for High-Performance Business, DELL PowerConnect J-Series Ethernet Switching Solutions: Building a Highly-Available Enterprise Network "A Dell Technical White Paper, 2010.Visited on 14 January 2017.

[17]. Cisco Systems, Inc., Delivering High Availability in the Wiring Closet with Cisco Catalyst Switches, White Paper, Dec 11, 2013. Visited on 14 January 2017.

[18]. The Availability Digest, Calculating Availability – Heterogeneous Systems Part 1, March 2008" http://www.availabilitydigest.com/public_articles/0303/calculating_availability_heterogeneous_syst.pdf", Visitedon 14 January 2017.

[19]. The Availability Digest, Calculating Availability – Redundant Systems, October 2006, http://www.availabilitydigest.com/public_articles/0101/calculating_availability.pdf, Visited on 14 January 2017.

[20]. System Reliability and Availability, http://www.eventhelix.com/RealtimeMantra/FaultHandling/system_reliability_availability.htm, Visited on 14 January 2017.

[21]. Zeng, Jihong. "A case study on applying ITIL availability management best practice." Contemporary Management Research 4.4 (2008).

[22]. Nickel, S.J, The Investment Decisions of Firms. Cambridge: University Press, 1978. Office of Government Commerce (2000). IT Infrastructure Library. The Stationary Office: London.

[23]. Zacks, S., Introduction to Reliability Analysis: Probability Models and Statistics Methods. New York: Springer-Verlag, 1992.

[24]. The Availability Digest, High Availability Network Fundamentals, April 2009, http://www.availabilitydigest.com/public_articles/0404/ha_networks.pdf, Visited on 14 January 2017.

[25]. E. E. Lewis, Introduction to Reliability Engineering, J. W. Sons, Ed. New York: Wiley, 1987.

[26]. Soleimani, Morteza, and Mohammad Pourgol-Mohammad. "Design for reliability of complex system with limited failure data; case study of a horizontal drilling equipment." Proceedings of the Probabilistic Safety Assessment and Management PSAM 12 (2014).

[27]. High Availability Network Operations, www.cisco.com/networkers/nw01/pres/pr/ps_presos/PS_544_1HANTULA_C3.pdf, Visited on 14 January 2017.

[28]. Desroches, Alain, and Sébastien Delmotte. "Macro-Cartographie des Risques par Audit: une méthode de diagnostic et de management global des risques d'entreprise." QUALITA'2015. 2015.

[29]. Desroches, Alain. "Notion de risque et approche de la maîtrise des risques." 6 et 7 avril 2011.

[30]. EU general risk assessment methodology (Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU, http://ec.europa.eu/DocsRoom/documents/15261/attachments/1/translations/en/renditions/native.”, 16 October 2015.

[31]. AIRMIC, Alarm, and A. IRM. "structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000." The Public Risk Management Association, London, UK (2010).

[32]. SP800, N. I. S. T. "Risk Management Guide for Information Technology Systems.", 2002.

[33]. Network Infrastructure Committee. "FTTH Infrastructure Components and Deployment Methods, 2007.".

[34]. Cale, Ivica, Aida Salihovic, and Matija Ivekovic. "Gigabit passive optical network-GPON." 2007 29th International Conference on Information Technology Interfaces. IEEE, 2007.

[35]. ABB, Reliability of uninterruptible power supplies, “https://library.e.abb.com/public/091b6999a8964a64b11331852879ca25/White_Paper_Relibility_150506.pdf” Visited on 15 January 2017.