World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:9, No:12, 2015

# Criticality Assessment of Failures in Multipoint Communication Networks

Myriam Noureddine, Rachid Noureddine

International Science Index, Information and Communication Engineering Vol:9, No:12, 2015 waset.org/Publication/10004411

***Abstract*—**Following the current economic challenges and competition, all systems, whatever their field, must be efficient and operational during their activity. In this context, it is imperative to anticipate, identify, eliminate and estimate the failures of systems, which may lead to an interruption of their function. This need requires the management of possible risks, through an assessment of the failures criticality following a dependability approach. On the other hand, at the time of new information technologies and considering the networks field evolution, the data transmission has evolved towards a multipoint communication, which can simultaneously transmit information from a sender to multiple receivers. This article proposes the failures criticality assessment of a multipoint communication network, integrates a database of network failures and their quantifications. The proposed approach is validated on a case study and the final result allows having the criticality matrix associated with failures on the considered network, giving the identification of acceptable risks.

***Keywords*—**Dependability, failure, multipoint network, criticality matrix.

## I. Introduction

THE concept of security is being integrated into all systems such as in the areas of industry, distribution, management of information and communication. Whatever the area and following the current economic challenges, all systems must be efficient and operational during their activity. So, to avoid an interruption of the system function, it is necessary to identify and evaluate their failures. This is to minimize the possible risks through the threshold of acceptable risk, defined following an assessment of the occurrence probability and the effects of failures severity. This double evaluation leads to a criticality estimation of the failures for any systems.

The considered system, in this work, is in the context of new information technologies especially in the communication networks. Given the evolution of this domain, the data transfer has evolved from a unicast to a multipoint communication. This transmission mode can simultaneously report information from a sender to multiple receivers.

This article deals with the failures criticality assessment of a multipoint communication network, by software that integrates a database of network failures and their quantifications. The validation of the proposed approach is obtained by its application on a multipoint network, giving the criticality matrices for each element of this system.

M. Noureddine is with the Department of Computer Science, University of Sciences and Technology of Oran, Algeria (corresponding author; e-mail: myriam.noureddine@ univ-usto.dz).

R. Noureddine is with the Institute of Maintenance and Industrial Safety, University of Oran 2, Algeria.

Section II presents the general notions related to the concept of failures criticality in a dependability context. The adopted approach for the failures assessment of a computer network is given in the next section. Section IV describes the application of the method on a network example following the different steps, with in the end the assessment of failures through criticality matrices.

## II. Failures Criticality

The dependability is the ability to deliver a service of confidence justified, i.e. the ability to avoid service failures [1]. Dependability concerns all the means which produce and maintain a certain level of trust in the success of an activity and its safeness [2]. Thus, the dependability, also known as science of failures [3] consists in controlling the failures and a failure is defined as the alteration or cessation of the ability of a device to perform a required function.

A system is failed if its functional capacities are interrupted (failure or voluntary shutdown) and then it is considered or declared incapable of ensuring the functions required by the operator.

The concept of risk refers to the concept of feared event or undesirable event, assessed in terms of frequency and severity [3]. In the dependability context, it is to identify undesirable events, that we are associated to the failures of the system.

### *A. Evaluation Approaches of Criticality*

The notion of criticality is fundamental in dependability because it allows quantifying the risks of failures, by assessing the frequency and severity of their occurrences. This evaluation is obtained through different methods.

The method of Pareto [4] is a statistical tool which allows identifying the relative criticality of historical data. It has the advantage of being easy and quickly implemented. But, the absence of interactions between the selection criteria represents a major drawback.

In the methods from the dependability domain such as the preliminary risk analysis, the failure trees, the failure modes effects and criticality analysis (FMECA), the reliability block diagrams, the criticality assessment is based on an analytical approach using the data from the return of experience [5].

The FMEA and the FMECA (FMEA with the criticality evaluation C) held an important place in dependability to identify and analyze potential failure modes of the various parts of a system and the effects of these on the system [6]. The criticality C is calculated from the consequence, the frequency and the detection of failures. So, this method allows identifying, prioritizing, and eliminating potential failures from the system [7]. The result is a structural decomposition

International Science Index, Information and Communication Engineering Vol:9, No:12, 2015 waset.org/Publication/10004411

and hierarchical of the system, as well as grids grouping the identified failure modes.

The Farmer diagram allows representing both the level of consequences and their frequency. It identifies the levels corresponding to a criticality domain. This diagram allows visualizing the domains with acceptable and unacceptable risks [8]. The boundaries between the zones are established by defining the thresholds for severity and frequency for each type of consequence considered. In the studies of dependability, the representation of the Farmer diagram by the criticality matrix is the most used method to take this problematic of the critical equipments hierarchy [9], [10].

### *B. Criticality Matrix Method*

Based on the principle of the Farmer diagram, the criticality matrix involves, instead of a linear border, a set of two values formed by the probability/severity beyond which the risk passes. This method follows the same approach as in the Probability-Impact matrix, which defined the relative importance of risks, through the evaluation both of the probability and the impact scores [11].

In the method of criticality matrix, the risk is assessed border from the acceptable area to the unacceptable area [9], [10]. According to the principle of the method, the evaluation of potential risks allows the criticality calculus, from the estimation of two factors: severity of the failure consequences "G" and their frequency of occurrence "F". Note than this criticality may also be expressed from three parameters, involving the detection parameter "D" and called the Risk Priority Number (RPN) [12], [13].

There are several scales for assessing the factors. For example, the quotations from 1 (the least critical) to 4 (most critical) are used for the severity parameter [14], an extra degree of criticality is added for the parameter "G" giving a scale from 1 to 5. The authors in [9], [12] uses a rating scale ranging from 1 to 6 for the two parameters "G" and "F". In the standard reference [15], the severity is classified in four levels, from the level 1 (catastrophic) to 4 (minor), and the frequency is classified in 5 levels (from A to E). Some authors use a rating scale ranging from 1 to 10 for the parameters like in [12], [16].

In the absence of a directive to establish a scale for the two parameters, from the standard reference and after synthesis, we adopt in this article an estimated value (Fig. 1) from the minor failure (value 1) to the catastrophic failure (value 4) for the severity rating and a scale of 1 to 6 for the frequency index.

## III. Proposed Approach

A multipoint computer network is an open full model for dissemination to a group of stations. This network system, called multicast technique [17], is a system where there is one sender and multiple receivers for the same transmission like in Videoconferencing.

Our approach to evaluate the criticality of the computer failures is formed of three sequential steps (Fig. 2): The functional decomposition of the network and then the identification and quantification of failures, grouped in the functional and dysfunctional analysis.

| **Frequency** | **Severity** | | | |
|---|---|---|---|---|
| | **1** : Insignificant | **2** : Marginal | **3** : Critical | **4** : Catastrophic |
| **1** : Frequent | | | | |
| **2** : Probable | | | | |
| **3** : Occasional | | | | |
| **4** : Faraway probability | | | | |
| **5** : Unlikely | | | | |
| **6** : Not credible | | | | |

Fig. 1 Criticality Matrix with the Adopted Factors

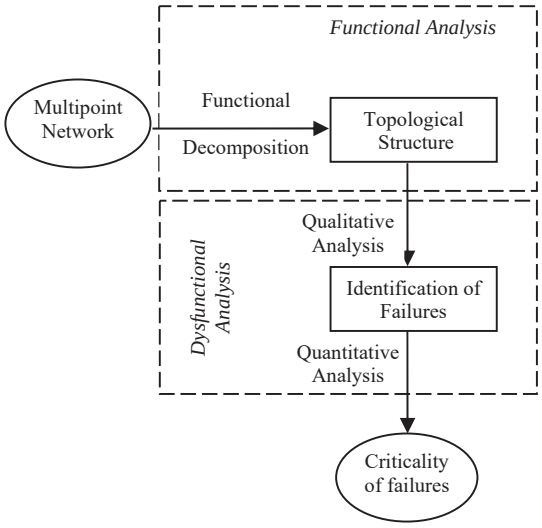


Fig. 2 Methodology Approach

### *A. Functional Analysis*

Upstream to the identification of failures, the functional decomposition step is necessary in order to decompose the system to determine its elements. We have applied the approach of functional analysis [18] which allows establishing the functional relationships to the interior and exterior of the systems. We use the functional decomposition following the FAST method (Function Analysis System Technique) [18]. This technique allows highlighting the design process by showing the relationship between need and solutions, though also the answers to the following three questions from a fundamental need clearly identified: Why? When? How? In the context of a multipoint network, the fundamental need is 'the sending of a set of messages to a group of clients'. The application of the FAST method gives the respective answers to the three previous questions: 'exchange and good movement of data or messages', 'when we want to access the data quickly and communicate effectively'. These responses are used to identify the following functions: the client sends a request to the server to receive messages, the server sends information

International Science Index, Information and Communication Engineering Vol:9, No:12, 2015 waset.org/Publication/10004411

and the client receives the data.

At the conclusion of this study, we obtain a functional diagram formed of three components: server, router and client. The server is the source supplying services to other programs or machines (for example, emission of messages); the router is software tool or equipment to route the data through the network; it can also designate an interface between two networks using different protocols. The client is a set of receivers or clients that can be put in a group. This approach allows finding the topological structure of this system, which is graphically represented by a media support nodes to the multipoint transmission and the leaves for the whole of the receivers [19]. We hold therefore the following elements (Fig. 3): A server, a set of routers, a set of receivers or clients who may be placed in a group and connecting links between these elements.

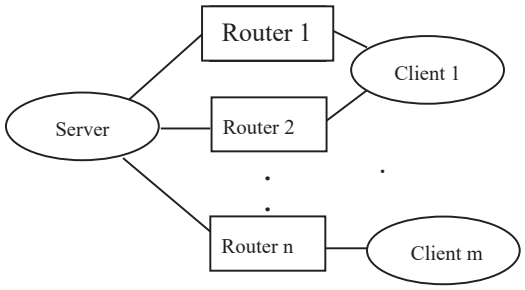


Fig. 3 Topological Structure of a Multipoint System

### *B. Dysfunctional Analysis*

For the identification of failures, the framework of FMEA approach is adopted. From the previous functional decomposition, the basic failures on the three components of the system (server, router and client) of the multipoint network are determined. Eighteen failures are listed, three failures on the router, and knowing that the server and the clients are considered such as computers, the others failures on these two last components will be the same.

In the adopted framework, the qualitative analysis allows the identification of failure modes and their effects, and the causes which are all of the events leading to the dysfunctional on an element of the system. The effect expressing the result of the failure, and these three concepts are related by the following relationship: 'Cause → Mode → Effect'.

Two generic modes are adopted namely "Loss Function" (LF) and "Degraded Function" (DF) giving the status of the network compared to a failure. In the same manner, two generic effects are identified namely 'Full Stop" (FS) and "DySfunction" (DS) to define the consequence of failure. So, each codified failure can be represented by a three-value record (Table I) according to its mode (LF/DF) and its effects (FS/DS).

Each failure is estimated following its seriousness and its index of occurrence frequency. The severity degree is estimated following the previous scale, (see last column in the Table I) from 1 to 4 and the index of occurrence frequency (from 1 to 6) is then dynamically assigns. These measures will use to generate the criticality matrix and to identify acceptable risks.

In the dependability context, failures can be classified [3], [7] according to the degree, the appearance speed or the combination of both (appearance speed and degree). The degree of failure is defined according to its amplitude i.e. the function is degraded or absent. It distinguishes between partial and complete failure. The appearance speed of a failure is defined according to the quickness of its manifestation. It distinguishes between sudden and gradual failure. The classification of failures as a function of degree and speed allows defining the catalectic failures (failure which is both sudden and complete) or failures by degradation (failure which is both gradual and partial). For example, on the router, the first record represents the failure 1 (cause: Unavailability of the ram) generating a loss function mode and giving a full stop of the router, with the maximum value for this failure severity. So, this failure is completed and it has a full degree.

The third record represents the third failure, generating a degraded function mode and giving a dysfunction of the router and in this case, this third failure is partial and it has a partial degree.

TABLE I
IDENTIFICATION OF QUANTIFIED FAILURES

| N° | Failure on the router (cause) | Mode | Effect | Severity |
|---|---|---|---|---|
| **1** | Unavailability of the RAM | LF | FS | 4 |
| **2** | Unavailability of the ROM | LF | FS | 4 |
| **3** | Saturation of the CPU | DF | DS | 2 |
| | Failure on the server/client (cause) | | | |
| **4** | Failure of the HD (hard drive) | LF | FS | 4 |
| **5** | Burns of the RAM | LF | FS | 4 |
| **6** | Short circuit power cable | LF | FS | 3 |
| **7** | Overvoltage of the motherboard | DF | DS | 2 |
| **8** | Damage network card | LF | FS | 4 |
| **9** | The LNA not authenticate | DF | DS | 1 |
| **10** | The LNA blocked | DF | DS | 2 |
| **11** | Malfunction of the LNA | DF | DS | 1 |
| **12** | LNA wrong | DF | DS | 4 |
| **13** | Stop graphics card | LF | FS | 3 |
| **14** | BIOS Password not recognized | LF | FS | 4 |
| **15** | Connection cable DD damaged | LF | FS | 3 |
| **16** | Sound card son not recognize | DF | DS | 1 |
| **17** | Power Switch Stuck | LF | FS | 4 |
| **18** | RAM failure | LF | FS | 4 |

## IV. CASE STUDY

### *A. The Network Specification*

The case study focuses on a network multi points [20] formed of a server (R), of 9 routers (Ri, i=1 to 9), and 3 groups of receivers (GRj, j= 1 to 3). There is only one transmission from the server to the group GR1 through the three routers R1, R2 and R3; the group GR2 can receive the data through three transmission paths, following the R1, R2, or R3, R4, R5 or R4, R7, R8. The group 3 receives the data of the connection formed in R5, R6, and R9 or of the connection formed of routers R6, R7. In the context of communication from a server to different clients, the connections are grouped together via

International Science Index, Information and Communication Engineering Vol:9, No:12, 2015 waset.org/Publication/10004411

the different routers in a path modeled by a diagram in series, noted RLk. So, there is one path RL1 for GR1, three paths for GR2 and two paths for GR3.

Fig. 4 gives the representation of the network following the server R, the three clients GR1, GR2 and GR3 with transmission paths RLi; a switch allows ensuring the dispatching of the information from the server. This implementation is obtained through software [21] developed and dedicated to the automatic generation of the criticality matrix.

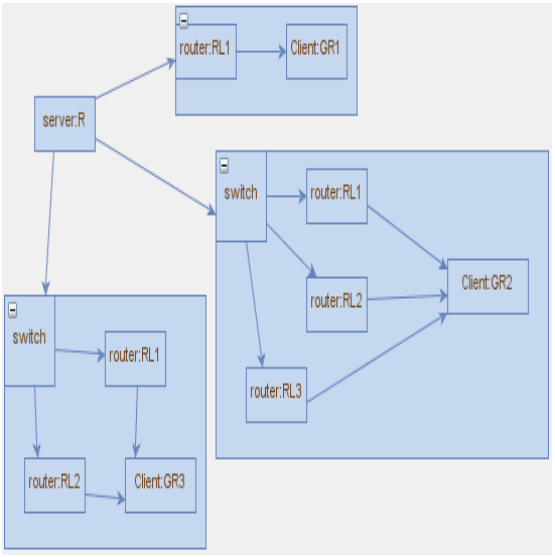


Fig. 4 Structural Description of the Network

### B. Database Failures

The set of failures identified and quantified previously is stored in a database. Fig. 5 shows a part of the database for the failures of a router (RL1).

In order to generate the criticality matrix, for each failure the index of frequency occurrence is dynamically assigned following the previous scale previously estimated. For example, for the two failures 1 and 3 on the router the factors of frequency are estimated at 3 because these failures do not exist often.

From the severity factors stored in the database and the frequency factors dynamically assigned, the criticality matrix is automatically generated after failure selection.

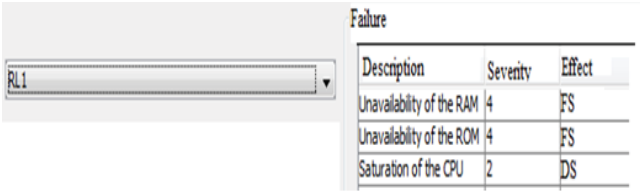


Fig. 5 Failures of the Router RL1 in the Database

We give some examples of failures showing the generation of the criticality matrix following the different components.

### C. Criticality Matrix on Router

Consider the two failures 1 and 3 on the router RL1 of group 2, corresponding to an unavailability of the ram and a saturation of CPU, with respective severity of 4 and 2 inducing a full stop and a dysfunction. The criticality matrix is generated automatically (Fig. 6) from these last values and from the factors of frequency estimated at 4.


Fig. 6 Criticality Matrix on Router

### D. Criticality Matrix on Server/Client

The two failures 4 and 7 on the server R are considered corresponding to a failure of the hard drive and to a power surge of the motherboard. Their severity degrees defined previously (in Table I) and stored in the data base are respectively 4 and 2. The criticality matrix is generated automatically (Fig. 7) from these last values and from the factors of frequency estimated respectively at 2 which shows that this failure is likely and to 3 because this failure occurs occasionally.

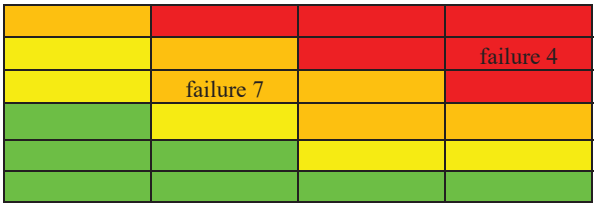


Fig. 7 Criticality Matrix on the server

Following the same approach, the three failures 15, 16 and 18 are considered, respectively corresponding to the damaged cable providing the connection of the hard disk, to the sound card not recognized and to a failure of the RAM card.

The criticality matrix is generated (Fig. 8) from the factors of severity given in Table I (stored in the database) and from the factors of frequency estimated respectively at 4, 1 and 2.


Fig. 8 Criticality Matrix on the client

### E. Result Interpretation

The criticality matrix associated to specific failures allows the identification of acceptable risks through a way that is visual and therefore immediate. Thus, in the three previous examples, there is no insignificant failure (not in the green

zone). On the other hand, there is unacceptable failures (in the red zone) as the failures 4 and 18 with catastrophic severity and which inducing a full stop of the network. The failures 1, 7, 15 and 16 are undesirable (orange area) and therefore, must be avoided: they correspond to a severity degree from 1 to 4, with a variable frequency and leading to a full stop or a dysfunction of the network. There is a single failure acceptable (yellow zone), the failure 3 of router and inducing a network dysfunction.

## V. Conclusion

This article has presented an assessment of the failure criticality for a multipoint network. Our framework is in the dependability context, and the adopted approach is formed of three sequential steps namely the functional decomposition of the network and then the identification and quantification of failures.

The two first steps are supported respectively by the FAST and the FMEA method. Each identified failure is therefore assigned with a severity degree and an index of occurrence frequency assigned dynamically. These factors are used to generate the criticality matrix and to identify acceptable risks.

The generation of the criticality matrix is automatic, implemented in software that integrates failures database of the network and their quantifications.

The whole approach has been applied to a case study through an example of computer network, where the failures have been identified and estimated. This evaluation allows generate the criticality matrix for the three elements of this communication system and finally, giving failures that will lead to the interruption of the data transmission.

Knowing that this work is a first step for the study of failures risks in a multipoint computer network, we are considering applying the approach on a real network computing in order to identify the effective failures with their respective degrees of severity and occurrence frequency. So, a history of evaluated failures will be generated and may prove very useful in the context of a predictive study of dependability in order to border the acceptable risks that may be involved in a computer network. On the other hand, the joint application of the FMCEA method by adding the criticality calculus will allow both to validate the result of acceptable risks and to reduce them by adding corrective actions.

This work also helps to show that the methods usually applied in dependability studies of industrial systems can also provide knowledge in dependability of computer networks.

## References

[1] A. Avižienis, J.C. Laprie and B. Randell, "Fundamental Concepts of Dependability", *UCLA CSD Report no. 010028, LAAS Report no. 01-145, Newcastle University Report no. CS-TR-739,* 2011.

[2] F. R. Chevreau, "Safety culture as a rational myth: Why developing safety culture implies engineering resilience", in *Proc. of the second resilience engineering symposium,* Antibes-Juan Les-Pins (France), 2006.

[3] A. Villemeur, *Sûreté de fonctionnement des systèmes industriels*, Eyrolles, 1988.

[4] F. Monchy, *Maintenance. Méthodes et organisation*, Dunod, 2000.

[5] G. Zwingelstein, "Evaluation de la criticité des équipements- Méthodes analytiques", *Techniques de l'ingénieur*, SE 4005, 2014.

[6] I. Elyasi-Komari, A. Gorbenko, V. Kharchenko and A. Mamalis, "Analysis of Computer Network Reliability and Criticality: Technique and Features", *International Journal of Communications*, *Network and System Sciences*, 4, 2011, pp. 720-726.

[7] M. Rausand and A. Høyland, System reliability theory. Wiley & Sons, 2004.

[8] C. Cremona, *Structural Performance: Probability-Based Assessment*. Wiley-ISTE, 2012.

[9] S. Kitazawa, K. Okayama, Y. Neyatani, F. Sagot, D. Houtte, L. Abadie, I. Yonekawa, A. Wallander and W.D Klotz, "RAMI analysis of ITER CODAC", *Fusion Engineering and Design,* 87(7-8), 2012, pp. 1510-1513.

[10] C. Ma, Z. Gao and L. Yang, "Safety analysis of airbone weather radar based on failure mode, effects and critically Analysis", *Procedia Engineering,* 17, 2011, pp. 407-414.

[11] A. Yazdani, S. Shariati and A. Yazdani-Chamzini, "A risk assessment model based on fuzzy logic for electricity distribution system asset management", *Decision Science Letters*, 3(3), 2014, pp. 343-352.

[12] Reliasoft, "Examining Risk Priority Numbers in FMEA**",** *Reliability Edge Home*, 4 (1), 1, 2003, pp. 14-16.

[13] N. Sellappan and K. Palanikumar, "Modified Prioritization Methodology for Risk Priority Number in Failure Mode and Effects Analysis", *International Journal of Applied Science and Technology*, 3 (4), 2013, pp. 27-36.

[14] P. Veras, P. Scherer, F. Silva, P.R.S. Barros and V.A. Santiago Junior, "FMEA as a Design Improvement Tool of protoMIRAX Attitude Control Subsystem," in LADC'2013, 2013, Rio de Janeiro (Brazil).

[15] MIL-STD, Procedures for Performing a Failure Mode, Effects and Criticality Analysis. *MIL-STD 1629A, Military Standard,* U.S. Department of Defense, 1980.

[16] K. Jenab and J. Pineau, "Failure mode and effect analysis on safety critical components of space travel", *Management Science Letters*, 5(7), 2015, pp. 669-678.

[17] J. Karvo, A study of teletraffic problems in multicast networks. *Dissertation for the degree of doctor of science in technology*, University of Technology, Helsinki (Finland), 2002.

[18] J.W. Bryant, "Function Analysis Systems Techniques: the basics", *Monograph of the SAVE International,* The value society, 1999.

[19] F. Arnal, Optimisation de la fiabilité pour des communications multicast par satellite géostationnaire. *PhD Thesis, Ecole Nationale Supérieure des Télécommunications,* Paris (France), 2004.

[20] M. Noureddine and S. Benhabib, "Performance et fiabilité des systèmes de communication multipoints", in *Proc. of the 10ème Congrès International de Génie Industriel (CIGI2013),* La Rochelle (France), 2013.

[21] N. Hadjioui, C. Habchi and M. Noureddine, Criticité des défaillances dans les applications multipoints. *Master Project in Computer Science*, University of Sciences and Technology of Oran (Algeria), 2011.

**Myriam Noureddine** is currently an Assistant Professor in the department of computer science, Faculty of Mathematics and Computer Science in the University of Sciences and Technology of Oran, Algeria. Among her research interests, the dependability domain is important dealing with the failure diagnosis, risk management and system reliability, with application in industrial systems and computer networks.

**Rachid Noureddine** is currently an Assistant Professor in the Institute of Maintenance and Industrial Safety, University of Oran 2, Algeria. He is interested in the maintenance domain with the industrial diagnosis, risk management and system reliability, with application in industrial systems and electromechanics system.

International Science Index, Information and Communication Engineering Vol:9, No:12, 2015 waset.org/Publication/10004411