A System of Systems Framework for the Reliability Assessment of Telecommunications Networks

Kosmas Tsilipanos, *Member, IEEE,* Ioannis Neokosmidis, and Dimitris Varoutas, *Senior Member, IEEE*

***Abstract*—In this paper, a system of systems (SoS) framework for the reliability analysis of telecommunication networks is proposed. In this framework, two hazard analysis techniques, hazard and operability analysis and fault tree analysis, are combined in a hybrid scheme. This is further enhanced using the Bayesian network model along with sensitivity analysis in order to answer complex probability queries and to estimate the impact of residual mishap risks, unknown events, or events that cannot easily be modeled. The SoS emergent behavior is further revealed using exploratory modeling. The proposed SoS framework is applied in the case of a fiber-to-the-curb VDSL telecommunication network.**

***Index Terms*—Bayesian networks (BN), conditional probability, fault tree analysis, fiber to the curb, hazard and operability analysis, residual mishap risk, system of systems (SoS), telecommunications.**

I. Introduction

BANDWIDTH-INTENSIVE applications requiring quality of service, such as video on demand, teleconferencing, live TV, and distributed simulations, are driving the net revolution toward delivering faster and highly reliable networks to the user. Service continuity is becoming a critical path for the delivered quality of service [1]. Toward this end, telecommunication companies are continuously investing in research and development for reliability analysis.

However, the provision of uninterrupted services that require high bandwidth and interactivity often leads to increased complexity of telecommunication systems. This converts the new generation of telecommunications networks into "systems of systems," consisting of a mixture of software, hardware, and human intervention.

The system of systems (SoS) concept is not new and it was initially introduced in the aerospace and defense areas [2]. However, in the last few years, SoS has been gaining increased attention as a means to accommodate the high complexity of metasystems. This concept can be applicable when a set of specific goals are fulfilled by mixing multiple systems. It should be noted that each of these systems can independently operate, but still need to interact with the others in order to achieve the common mission [2]. Some more contextual definitions of SoS are as follows.

1) An SoS involves the integration of multiple, potentially previously independent, systems into a principal level supersystem in order to carry out a mission for which each component plays an essential role but by itself is not capable of completing [3].
2) An SoS is composed when most of the following five critical characteristics are present: operational and managerial independence, geographic distribution, emergent behavior, and evolutionary development [4].

Boardman and Sauser summarized more than 40 different definitions and extracted the five main properties that an SoS should have: autonomy, belonging, connectivity, diversity, and emergence [5], [6]. It should be noted that due to the above properties, SoS are highly complex and exhibit dynamic and emergent behavior. The complexity is mainly due to the capability of the elements to operate independently while the emergent and dynamic behavior is a result of adding new systems or replacing older ones on the fly.

In the literature, numerous reliability studies can be found regarding several systems, such as power systems, software systems, and control and automation systems. In these traditional analysis techniques—some with slight modifications in order to match in the research field—such as hazard and operability analysis (HAZOP) [7], [8], fault tree analysis (FTA) [9]–[11], and Bayesian networks (BN) [12], [13] were used in order to reveal known hazards and risks that affect the safety and the performance of the systems under investigation. Traditional hazards analyses were initially designed to deal with system analysis rather than SoS analysis. Each one of the existing hazard analysis tools proved insufficient to deal with the complexity, geographical distribution, uncertain environment of operation, and the size of modern telecommunication networks. Hence, a new SoS framework combining known techniques should be investigated.

The starting point for the development of a new framework is to identify its requirements. The SoS framework should primarily address the high complexity, the large size, and the dynamic and emergent behavior of telecommunication networks. Moreover, it needs to be flexible to incorporate and evaluate the impact of unknown events. Recently, SoS software safety [14] has been investigated using a mixture of two slightly modified versions of the well-known techniques: HAZOP and network analysis [15] along with the goal question metric (GQM) approach of Basili [16]. However, this

Manuscript received September 18, 2011; revised March 20, 2012; accepted May 29, 2012. Date of publication September 4, 2012; date of current version February 20, 2013.

The authors are with the Department of Informatics and Telecommunications, University of Athens, Athens 15784, Greece (e-mail: ktsilipanos@di.uoa.gr; i.neokosmidis@di.uoa.gr; d.varoutas@di.uoa.gr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSYST.2012.2207274

1932-8184/$31.00 © 2012 IEEE

mixture was adapted to software safety and cannot be directly applied to telecommunication networks. Furthermore, only one type of hazards, interface hazards, can be investigated using the method proposed in [15]. It should also be noted that the effort of [15] to study the impact of "known unknown" and "unknown unknown" events was limited to qualitative results obtained by network analysis (using MIL-STD-882D). Quantitative results regarding the validation of the software safety requirements sufficiency are also presented using GQM approach along with the goal structuring notation. However, increased attention should be paid since GQM is a subjective method based on data collected from answers of stakeholders.

A very recent and serious effort dealing with uncertainty was also performed in [17] and [18]. In [17], a new reliability analysis technique was proposed. Uncertain parameters were modeled as random variables, while some distribution parameters are given variation intervals (strips). On the other hand, a hybrid model or data-based probabilistic design approach was proposed in [18] for the design of robust nonlinear systems under situations of parameter variation and model uncertainty. However, these models can be effective in partially unknown systems failing to address deep uncertainty. Furthermore, the proposed models are static and thus cannot be applied in SoS modeling in order to describe SoS emergent behaviors.

In this paper, a new SoS framework for the reliability assessment of telecommunication networks is presented. The proposed framework is a combination of the analytical method of HAZOP with the mathematical representation of FTA along with the directed acyclic graphs (DAG) of BN. In addition, this method encapsulates sensitivity analysis techniques (Monte Carlo simulations) in order to quantitatively evaluate the impact of unknown risks and events, such as the addition of new systems with unknown characteristics. In order to further reveal real SoS behaviors (e.g., evolution—emergent behavior of SoS), exploratory modeling is implemented. Numerical evaluations of model outcomes across a large set of possible SoS representations are performed giving the "whole picture" of SoS in a time sequence of different periods.

To the best of authors' knowledge, this is the first time that such a framework is proposed and used for the reliability assessment of telecommunication networks. The proposed framework proved useful in the determination and evaluation of known events, risks and hazards, as well as in the estimation of the impact of unknown events and the emergent behavior of the SoS.

The HAZOP and FTA techniques slightly modified by simply reducing the details during recording the hazards in order to address the complexity and scalability of the SoS under investigation. Contrary to other studies, the hybrid HAZOP-FTA scheme proceeds with the evaluation of the probability of failure of each system as well as of SoS. Additional metric, such as cut sets (CS) importance and risk reduction worth, are also estimated to quantitatively characterize the robustness of the SoS. Furthermore, it is applied without being trapped in specific hazards and failures such as dependent failures [19] and without making common assumptions used in the literature such as nodes with equal probability or failures coming only from links [20], [21]. The reduced accuracy of the modified hybrid scheme identified with the use of BN model. BN supports the reliability study framework by employing the use of complex probabilistic queries. In this paper, the BNs identify not only the service outage as in [21] but also the performance degradation. The analysis of [22] and [23] is further expanded by incorporating the impact of unknown events and hazards or complex events, such as rerouting and restoration [24], that are difficult to be modeled. Numerical results are also obtained describing the evolution of the SoS.

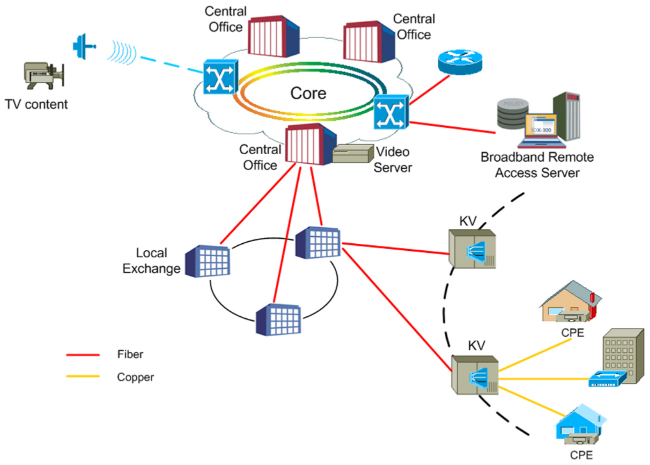


Fig. 1. System under investigation.

The remainder of this paper is organized as follows. In Section II, the SoS nature of fiber to the curb (FTTC) access networks is summarized. Section III presents the SoS framework proposed for the reliability analysis of such FTTC networks. The results obtained by the application of the hybrid technique along with the Bayesian model are presented and discussed in Section IV. Conclusions are given in Section V.

II. Network as an SoS

The telecommunication network under investigation is a FTTC access network based on the VDSL technology (Fig. 1). Before proceeding to the analysis of the proposed framework, one needs to answer the question of whether a VDSL network is, in fact, an SoS. As shown in Fig. 1, the network has five independent systems: the customer premises equipment (CPE), the digital subscriber line access multiplexer (DSLAM), the local exchange (LE), the central office (CO), and the broadband remote access server (BBRAS).

Human interaction should also be taken into account as a separate system in terms of administration and installation of the components. Software is considered as the seventh system since it is running in all platforms to support the applications. The systems under investigation are characterized by increased complexity, nonlinear behavior, and operation in uncertain environments. In the case of LE for example, the above characteristics are attributed to a large number of constituent components. More specifically, the LE consists of air conditions, power supply units, batteries for the UPS, switches, and so on. All these components are assembled into the LE in order to connect the backbone network to the access network.

TABLE I
HAZOP WORKSHEET

HAZOP Analysis									
No.	Item	Function/Purpose	Parameter	Guide Word	Concequence	Cause	Hazard	Risk	Recommendation

On the other hand, the physical medium (fiber, wireless, twisted pair) is of great importance for the proper operation of the telecommunication network allowing the different systems to connect and exchange information with each other. As this medium of communication has interfaces with each of the individual systems, it decisively affects their operation in terms of the overall performance.

Therefore, it is evident that each of the constituent systems can operate independently, performing a particular task. However, these systems can be combined together in a way to achieve a higher level mission, which is the provision of high data rates and advances services. Each of the systems plays its own important role in the SoS mission. Although each of the systems can have its own administration in order to deliver in a safe manner the services that it designed for, or there is a possibility of collocation of the incumbent and the alternative providers with more management centrals, these SoS should be better characterized as directed SoS. Hence, in the SoS under investigation the component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose [4]. Geographical distribution is also present in telecommunication networks. The distances between network nodes are in the order of a few tens of kilometers, and the information is transmitted from one component to another in order to provide the end user with connectivity at high data rates. Finally, the characteristic of evolutionary development is satisfied due to technological progresses. Based on the above analysis, it can be concluded that the network (hardware, software, and humans) under investigation lies perfectly on the given SoS definitions.

III. Hybrid Hazard Analysis Method

In the proposed analysis, HAZOP is initially combined with FTA. The resulting hybrid technique contains the advantages of both HAZOP and FTA, enabling the mathematical representation of the whole problem and the estimation of the probability of failure of both the constituent systems and SoS. A failure is defined as the state or event in which the system cannot totally (loss) or partially (performance degradation) deliver a promised service [25]. Given the above definition, the probability of failure can be directly related to the number of affected users.

However, it should be noted that the detailed HAZOP and FT analysis could not be applied successfully in the case of SoS under investigation. This is because the identification of the complete hazards list and of the residual mishap risks is a very complicated task, which becomes more difficult as new components (systems) and technologies are added to SoS. Hence, both techniques are slightly modified (coarse reliability analysis) by reducing the details of the hazards recording phase in order to become more flexible.

In the next step, the proposed analysis incorporates a BN model in order to take into account unknown events [26] or procedures that cannot be easily modeled due to their increased complexity. Using this model along with sensitivity analysis, one can evaluate special conditional probabilities that are critical for the reliability assessment of telecommunication networks. For the sensitivity analysis, identically distributed independent random variables are used. This can be avoided by using maximum entropy and least-squares error methods as proposed in [27], leading however to an undesired increase of complexity.

A. *HAZOP Analysis*

HAZOP [28] analysis is a well-structured qualitative technique. It allows the organized study of a system in detail in order to identify hazards that prevent its efficient operation. This method includes a systematic process for investigating possible operational deviations. Moreover, proper safeguards are used or proposed to prevent hazards from occurring. The HAZOP analysis is based on special adjectives (guidewords), such as “more,” “no,” “less,” and system conditions such as “speed,” “flow,” “pressure.” Although it is a relatively simple process, a multidisciplinary team headed by an experienced leader with deep knowledge of the system under study is required. Furthermore, there are rigorous steps that must carefully be followed to properly apply the described method.

In order to execute the HAZOP analysis, a specialized worksheet should be established. Since HAZOP analysis is a structured technique, a matrix or column-type worksheet should be used. The steps followed during HAZOP along with events and items are recorded in the worksheet.

A suggested HAZOP worksheet is illustrated in Table I. It can be deduced that such a worksheet must include key entries such as the following:

1) no: this column is needed for the reference to any part of the analysis;
2) item: it describes the component analyzed;
3) function or purpose: the component’s purpose or function in the system;
4) parameter: system parameter that will be evaluated;
5) guide word: the selected guideword for the analysis;
6) consequence: direct effect of the occurring guide word;

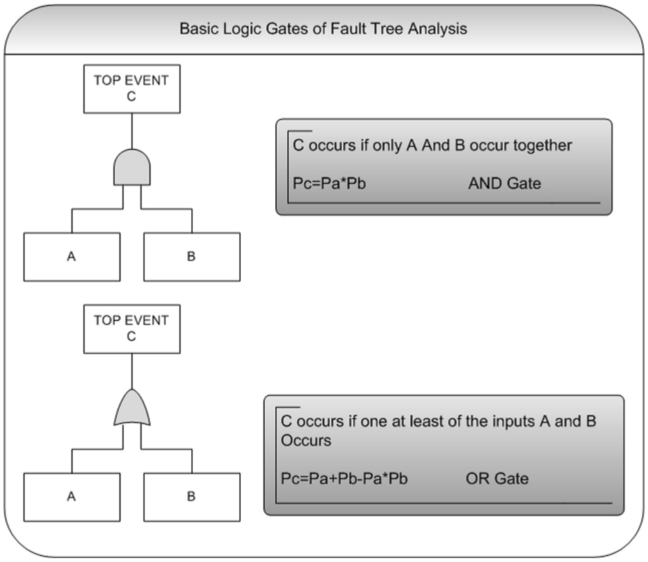

Basic Logic Gates of Fault Tree Analysis
TOP EVENT C
A
B
C occurs if only A And B occur together
Pc=Pa*Pb
AND Gate
TOP EVENT C
A
B
C occurs if one at least of the inputs A and B Occurs
Pc=Pa+Pb-Pa*Pb
OR Gate

Fig. 2. Logic gates used in the FTA.

7) cause: possible factors that lead to a specific deviation from normal operation;
8) hazard: hazard caused by the specific deviation;
9) risk: qualitative measure of mishap risk;
10) recommendation: recommendations for hazard mitigation.

B. FTA

FTA [28] is a graphical systems analysis technique using logic block diagrams that display the system state (top event) in terms of the states of its components (basic events). FTA is a quantitative technique, employed to evaluate large complex systems in order to early track and prevent possible problems. FTA is a top-down approach, and with the use of logic gates it quickly identifies the root cause along basic events. The use of logic gates also enables the development of a mathematical model, allowing the mathematical representation of the problem and the estimation of failure probabilities. FTA is relatively easy to perform and understand. The basic logic gates that are used for the analysis are depicted in Fig. 2.

FTA building is an iterative process of standard questions. The key products of the FTA are the CSs that identify the component failures and various combinations causing the occurrence of top events. Essentially, CSs reveal both the critical and weak links in a system analysis by demonstrating the safety problems. In general, a low order CS is a clear indication of a high risk. The generation of CSs requires the exploitation of specific algorithms that use the Boolean reduction (BR) technique. With BR the FTA events and branches that happen in more than one place are not accounted in the top event probability calculation. Some basic measures used in the FTA are presented in Table II.

TABLE II
FTA BASIC METRICS

Metric	Definition	Value and Notes
CS importance (I)	Evaluates the contribution of minimum CS to the top event (total) probability, $I_{cs}=P_{cut\_set}/P_{\text{total}}$	The highest the ratio, the highest the impact to the total probability $I_{\text{cs}} > 0$
Fussell–Vesely (FV) importance (I)	Evaluates the contribution of each event to the top event (total) probability, $I_{FV}=P_{event}/P_{total}$	The highest the ratio, the highest the impact to the total probability I_{FV} >0
Risk reduction worth (RRW)	Evaluates the decrease in the FT top event (total) probability if a given event A is guaranteed not to occur (set P_A=*0* in FTA)	High decrease in the total propability indicates critical event, 0<=RRW<=1
Risk achievement worth (RAW)	Evaluates the increase in the FT top event (total) probability if a given event A occurs (set P_A=*1* in FTA)	High increase in the total propability indicates critical event, 0<=RAW<=1

For the mathematical representation of the probability of failure P_A of component A, the exponential distribution of (1) is used

$$P_A = 1 - e^{-\lambda T} \tag{1}$$

where T is the component's exposure time and λ is the component's failure rate, which can be written as a function of the mean time between failures (MTBF)

$$MTBF = \frac{1}{\lambda}. \tag{2}$$

The constant failure rate and the memoryless property of the exponential distribution will help to avoid adding complexity in the proposed framework.

C. BN

BN [29] belong to probabilistic graphical models. These structures are used to represent specific knowledge in an uncertain domain. BN combine general principles from probability theory, graph theory, and statistics. A set of random variables (nodes) along with their conditional dependences (edges) are connected through a DAG. The nodes are drawn as circles each with a label corresponding to variable's name, while edges are represented by arrows showing the dependence of the connected nodes.

The graphical-qualitative representation of BN is usually followed by the quantitative part of the model. This includes parameters such as the conditional probability distribution at each node. It should be noted that BN must satisfy the Markov property, i.e., each variable depends only on its parents. The conditional probability is usually given in a table format, reporting the probability of the variable represented by the node for each combination of values of the node's parent variables.

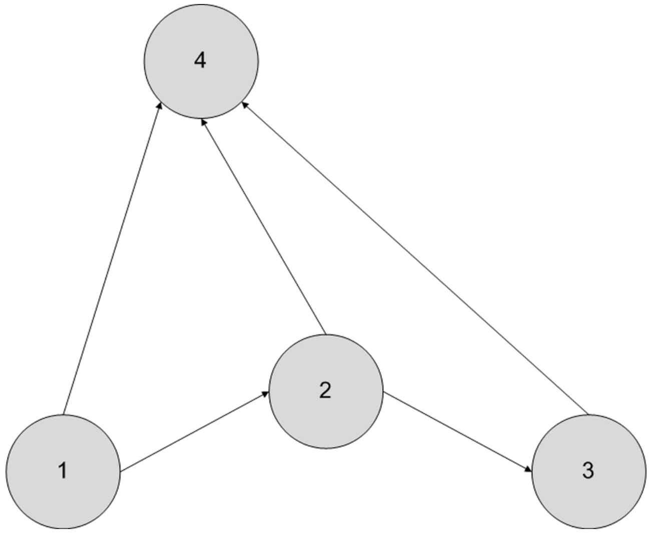


Fig. 3. BN model.

Hence, a BN can be defined by a set of nodes (random variables) $X = X_1, \ldots, X_\mathrm{n}$ with interdependences through a DAG G. The graph G corresponds to a joint probability distribution over the set of random variables

$$P\left(X_{1,}X_2, ..., X_n\right) = \prod_{i=1}^{n} P\left(X_i|P_a\left(X_i\right)\right) \qquad (3)$$

where $P_a\ (X_i)$ are the parents of X_i.

Consider, for example, the BN of Fig. 3, where node 3 is a direct cause of node 2, node 4 depends on nodes 1, 2, and 3 while node 1 has no parents. For each realization of each node conditioned on the set of its parents in the graph G, the conditional probabilities $\Theta P_r(2|1)$, $P_r(3|2)$, $P_r(4|1, 2, 3)$ should be evaluated. The DAG G over the set of variables $X(1, 2, 3, 4)$ is called a network structure, while Θ, also called network parameterization, is a set of conditional probability tables (CPT), one for each variable.

IV. Results and Discussion

A. Coarse Reliability Analysis

In this section, a coarse reliability analysis will be performed. This includes HAZOP and FT analysis by taking into account the absolutely necessary components of each system. In this case, residual mishap risks are incorporated using sensitivity analysis of a random variable.

The starting point of the hybrid analysis tool is the collection of the participant components along with their interconnections and interdependences. Then, the parameters and guidewords used in HAZOP are defined and recorded in the worksheet form, as shown in Table III. The HAZOP table for the CO reveals its main functionality within SoS, which is switching among LE subscribers. Furthermore, it is connected to BBRASs in order to get the required authentication through an optical fiber. However, this can be interrupted due to a failure or a mishap in the BBRAS or due to a fiber cut.

The HAZOP is repeated for each component separately and FTA follows to graphically represent the root cause of each top event. As shown in Fig. 4, the three parameters, connection, electricity, and temperature, can be triggered by hardware, software, or human errors.

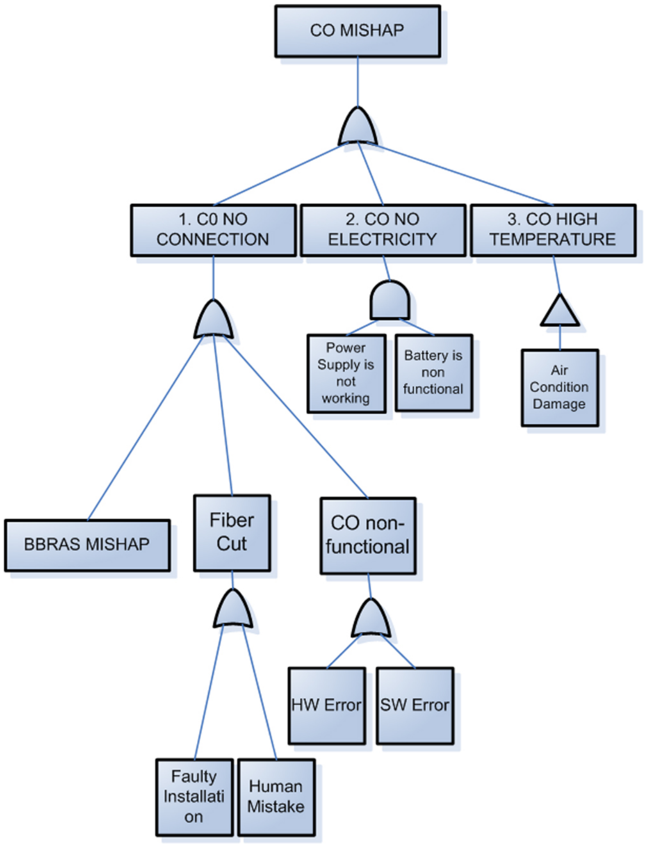


Fig. 4. FTA in the case of the LE.

In order to mathematically represent the block diagram of FTA, MATLAB's simulink toolbox along with Boolean algebra was used. As an example, the simulink model for the CO is illustrated in Fig. 5. Highlighted is the BBRAS mishap that acts as the interface hazard. The input parameters of the obtained model are the exposure time T and the failure rate λ that is the inverse of the MTBF. In this paper, the exposure time T is considered arbitrarily as 10 years. However, any other value of the exposure time can be easily introduced in the proposed framework. The MTBF, which was used in this paper, has been mined from the database of a built-in techno-economic tool containing numerous network components [30].

The probability of failure of each system is then estimated. As shown in Fig. 6, the BBRAS is the most reliable system, while the CPE is characterized by the highest probability of failure. The above result is somewhat expected since the BBRAS is located in a higher position in the network hierarchy compared to the CPE. This means that BBRAS serves numerous end users, while CPE is located at the customer's premise serving just one. Hence, BBRAS has to be more robust since its failure results in significant effects in terms of disconnected end users.

In order to evaluate the probability of failure of SoS, one should carefully investigate the relationships between the constituent systems. From Fig. 1, it can be deduced that the systems comprising SoS are connected in series. Therefore, an

TABLE III
HAZOP SPREADSHEET FOR THE CENTRAL OFFICE

No.	Item	Function/purpose	Parameter	Guide word	Consequence	Cause	Secondary cause	Hazard
1	CO	Serves switching among LE subscribers	Connection	NO	All assigned LEs not connected	BBRAS MISHAP		
						Fiber cut	Faulty installation	BBRAS–CO interface damage
							Human mistake	
						CO nonfunctional	Hardware error	CO equipment fault
							Software error	
2			Electricity	NO	All assigned LEs not connected	Power supply is not working		Loss of power
3			Temperature	HIGH	All assigned LEs not connected	Air condition damage		Equipment damage

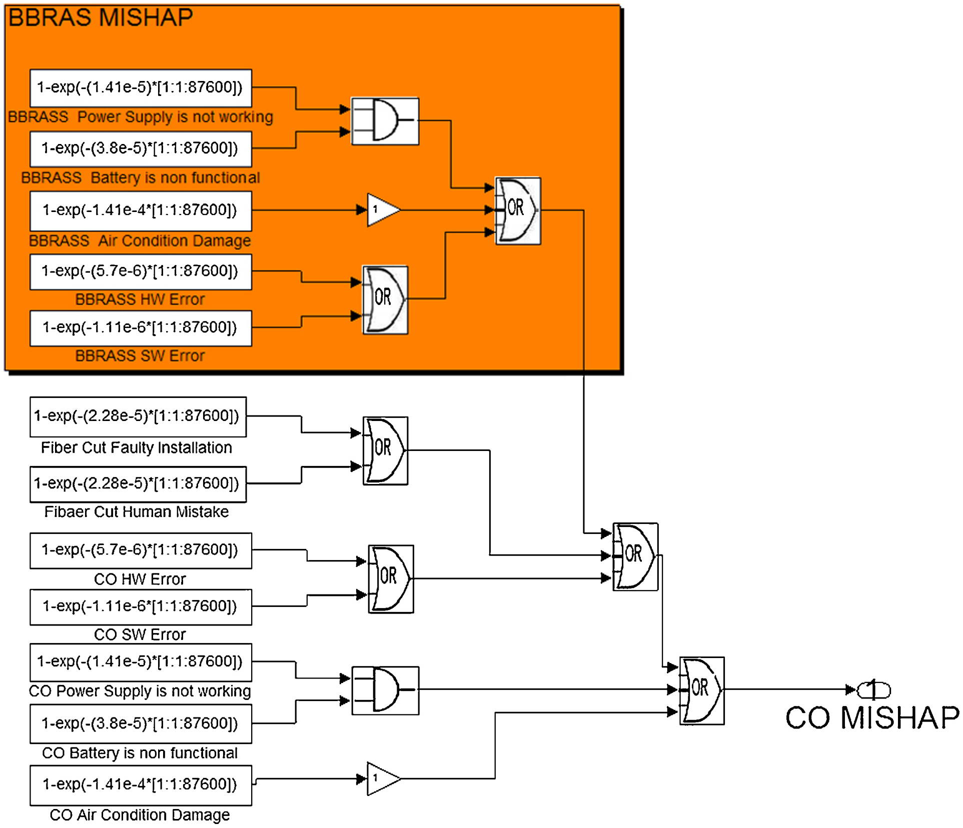

BBRAS MISHAP
1-exp(-(1.41e-5)*[1:1:87600])
BBRASS Power Supply is not working
1-exp(-(3.8e-5)*[1:1:87600])
BBRASS Battery is non functional
1-exp(-1.41e-4*[1:1:87600])
BBRASS Air Condition Damage
1-exp(-(5.7e-6)*[1:1:87600])
BBRASS HW Error
1-exp(-1.11e-6*[1:1:87600])
BBRASS SW Error
1
OR
OR
1-exp(-(2.28e-5)*[1:1:87600])
Fiber Cut Faulty Installation
1-exp(-(2.28e-5)*[1:1:87600])
Fibaer Cut Human Mistake
OR
1-exp(-(5.7e-6)*[1:1:87600])
CO HW Error
1-exp(-1.11e-6*[1:1:87600])
CO SW Error
OR
OR
1-exp(-(1.41e-5)*[1:1:87600])
CO Power Supply is not working
1-exp(-(3.8e-5)*[1:1:87600])
CO Battery is non functional
1-exp(-1.41e-4*[1:1:87600])
CO Air Condition Damage
1
OR
1
CO MISHAP

Fig. 5. Simulink model for the estimation of the CO probability of failure.

OR gate [31] must be used in order to evaluate the probability of failure of SoS, as shown in Fig. 7. However, increased attention should be paid during calculations. Multiple occurring events and branches observed in the FTA must be removed in order to avoid errors that will decrease the accuracy of the obtained results.

In the initial coarse analysis, the probability of failure of SoS equals the probability that at least one user does not enjoy the provided service. Therefore, the probability is identical to the probability of failure of the CPE due to the serial connection of the constituent systems. However, a different definition of the probability of failure of SoS could alter the above case. According to this definition, the probability of failure should depend on the number of disconnected users.

It is interesting to note that different SoS mishaps lead to different results in terms of the disconnected users. An SoS mishap coming from a hardware error of the CPE results in the disconnection of a single user. A mishap for the network that has to do with the LE will influence a serious number of connected DSLAMs, which affect multiple users. Although the results obtained from the coarse analysis are not of great importance, it gives us a first insight into the performance of SoS.

In the above analysis, the residual mishap risk as a result of a nonperfect hazard analysis in not accounted for. In order to incorporate the residual mishap risk, a random variable is introduced. In order to retain the complexity of the framework in low levels, the random variable is chosen arbitrarily to follow the normal distribution. It should be noted that the position of the residual mishap risk is significant. As expected, the introduction of the residual mishap risk in the CPE region (Fig. 6) has the maximum impact on the performance of SoS.

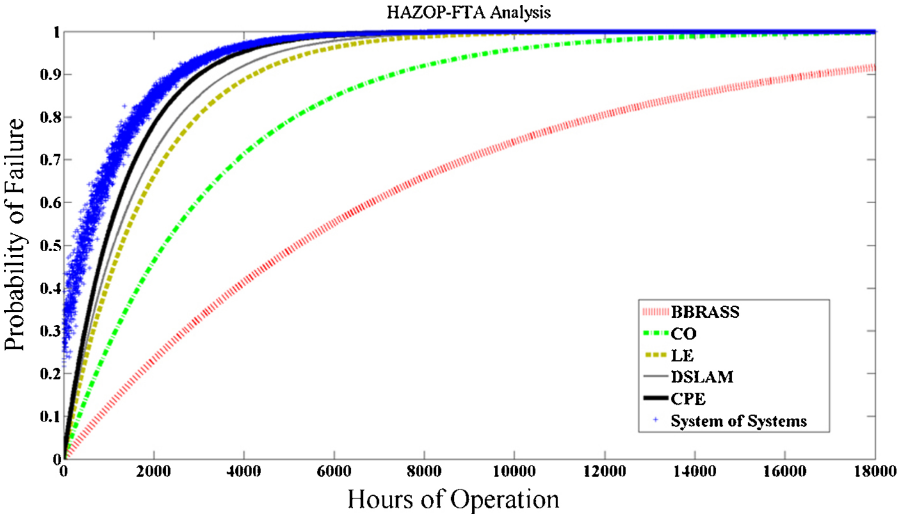


Fig. 6. Probability of failure of the SoS constituent systems for 18 000 h of operation.

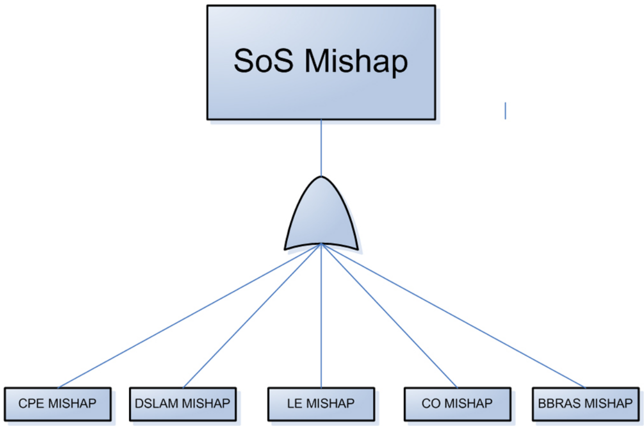


Fig. 7. SoS mishap.

Apart from the probability of failure, several importance metrics can also be derived through FT analysis. These metrics can be used to determine the significance of the contribution of all events in the FT to the probability of the top event. The first metric is the CS importance that equals the ratio of the CS probability to the FT top probability. The CS importance in the case of SoS is depicted in Fig. 8. It can be deduced that the "air condition fault or damage" event has the highest impact ratio in the SoS probability of failure and can be characterized as a critical event. This is not surprising since the air condition has the lowest MTBF.

The impact of lower level events can also be evaluated using the risk reduction worth (RRW) metric. This corresponds to the decrease in the probability of the top event if the lower level event did not occur. The RRW measure in the case of SoS is illustrated in Fig. 9. A conclusion similar to that of Fig. 8 can also be derived from the zoomed version of the RRW diagram. The omission of "air condition fault or damage" event results in the biggest reduction of SoS probability of failure.

Similarly, the importance metrics of the constituent systems can also be estimated in order to early track critical events and the high risk hours of operation.

B. Complex and Unknown Events

The above picture of a coarse analysis completely changes if one wants to incorporate additional information in the proposed framework. However, one should always have in mind the basic purpose of an SoS framework that is to address complexity and size issues while simultaneously maintaining its dynamic and emergent behavior. Thus, the inclusion of details should be performed in a general way to avoid overloading the proposed framework.

To begin with, the term "additional information" includes both unknown risks and events, which cannot be easily modeled, quantified, and described in precise terms. In the second set, one can incorporate failures on specific ports or elements that are not taken into consideration, such as the existence of backup systems, the ability of traffic rerouting [32], and the possibility of fast restoration [33]. In other words, the latter set of information mainly includes those actions that prevent failures before perceived by the end user.

Therefore, it is obvious that under this new perspective, one must ignore the rigorous block diagram of Fig. 1. Both the first and the second set of additional details may be connected either in series or in parallel with existing systems.

In order to incorporate complex and unknown events as well as to extract useful guidelines, one should resort to BN models. Such models will provide us with the asset of answering complex probabilistic queries about the network operation, using the information about nodes and interfaces obtained from the HAZOP and FT analyses. The BN describing the FTTC network under SoS perspective is shown in Fig. 10. Systems connected in parallel are used to represent the complex and unknown events. Unlike common serial-parallel reliability analysis, the inclusion of BN in the framework of the study makes feasible the generation of quantitative results that deal with complex and unknown events. This way, deep uncertainty is also modeled through the proposed framework.

A first insight into the impact of unknown or complex events and risks is the change occurred in the BN parameters, such as the CPTs of each system. By ignoring complex and unknown

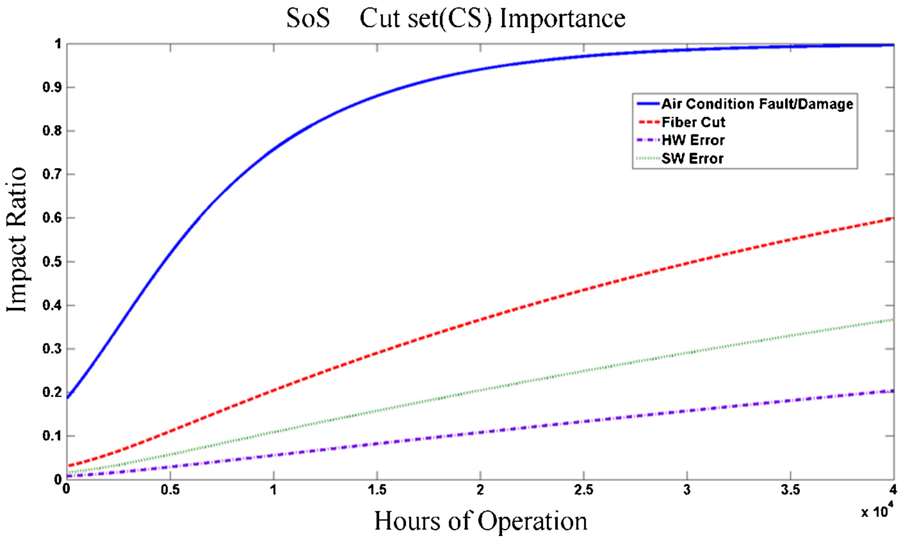


Fig. 8. Cut sets importance in the case of SoS.

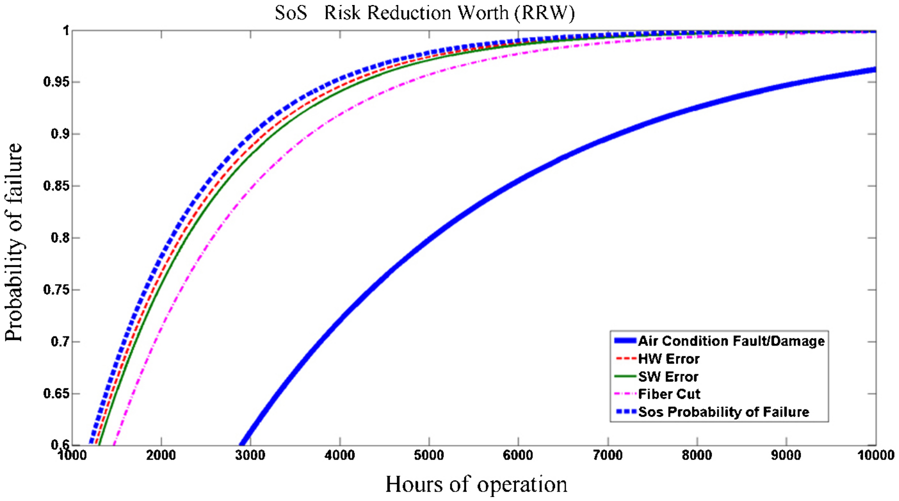


Fig. 9. Estimation of RRW for SoS.

TABLE IV
BN PARAMETERS FOR THE CO

Conditional Probability Table	BBRASS	
CO	Mishap=True	Mishap=False
Probability of Mishap=True	1	1-exp(-(0.0003124)*T)
Probability of Mishap=False	0	exp(-(0.0003124)*T)

events, the CPT for the CO is shown in Table IV. As shown in Table IV, the probability of failure of CO when the BBRAS has a mishap is equal to 1, which means that CO will also fail because of the interface hazard. On the other hand, when BBRAS has no mishap, CO probability follows an exponential function that is derived from the HAZOP-FTA analysis, as shown in Fig. 6. However, the incorporation of the parallel system at BBRAS level completely changes the CO's CPT. The BBRAS failure will not be transferred to the CO level since the service continuity is guaranteed through the parallel system.

Using the BN of Fig. 10, one can calculate several conditional probabilities, such as the probability of failure of the SoS given that LE is failing

$$P\,(SoS = True|CPE,\ DSLAM,\ LE = True,\ CO,\ BRASS) = \\ = \frac{\sum_{C,D,CO,B\in[True,\ False]} P(SoS{=}T,\,C,\,D,\,L{=}T,\,CO,\,B)}{\sum_{SoS,C,D,CO,B\in[True,\ False]} P(SoS,\,C,\,D,\,L{=}T,\,CO,\,B)} \tag{4}$$

where CPE, DSLAM, LE, CO, BBRASS, true, and false are written as C, D, L, CO, B, T, and F for simplicity.

Since the probabilities of failure of the parallel systems are unknown, one should resort to identically distributed random variables. However, in order to focus on the impact of the parallel to the LE system, its probability of failure ranges from 0.2 to 0.8, while the probabilities of failure of the others are chosen equal to 0.5 arbitrarily. In Fig. 11, the conditional probability of (4) is illustrated for three different sets of operation hours for the SoS.

From Fig. 11, it can be deduced that in the initial stages of SoS operation, the impact of the parallel to the LE system is higher. It is interesting to note that the SoS conditional probability marginally changes for more than 10 000 h of operation. In addition, as expected, the SoS conditional proba-

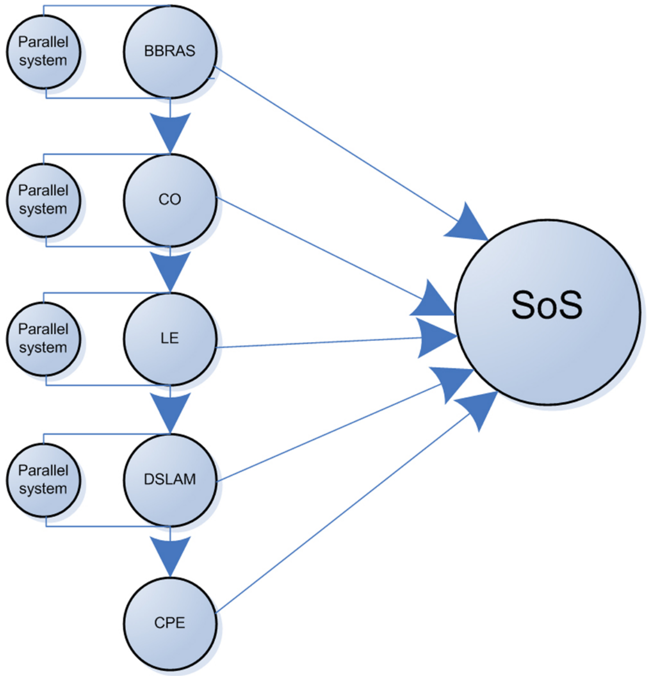


Fig. 10. Bayesian model for the SoS interconnection.

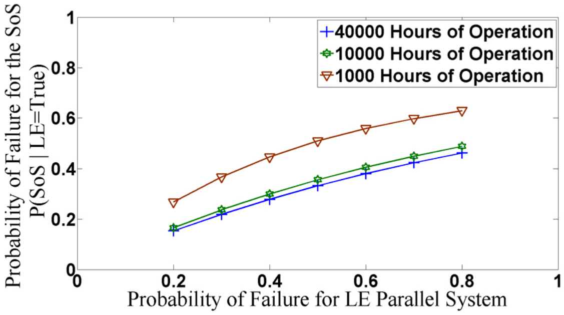


Fig. 11. Conditional probability of (4) for three different sets of operation hours as a function of the probability of failure of the LE's parallel system.

bility increases as the probability of failure of the LE's parallel system increases.

In order to further reveal the impact of simultaneously changing the probability of failure of the parallel systems, one can resort to Monte Carlo simulations. In Fig. 12(a) and (b), the histograms of the conditional probability of failure values [estimated using (4)] are shown for 10 000 h of SoS operation. These are obtained when the probabilities of failure of the parallel systems are randomly chosen from (a) a normal and (b) a uniform distribution inside [0.3, 0.7]. The conditional probability values for both distributions were calculated using 10^5 Monte Carlo iterations. It is interesting to note that the conditional probability exhibits an almost similar sensitivity for both distributions. In both cases, an SoS probability of failure equal to 0.35 is the most probable one. It can also be observed that the performance of the SoS is relatively prone to uncertainty-induced changes.

Figs. 11 and 12 provide an indication of the reliability of the obtained results against uncertainties in the incorporation of unknown events and risks or events that cannot be easily modeled.

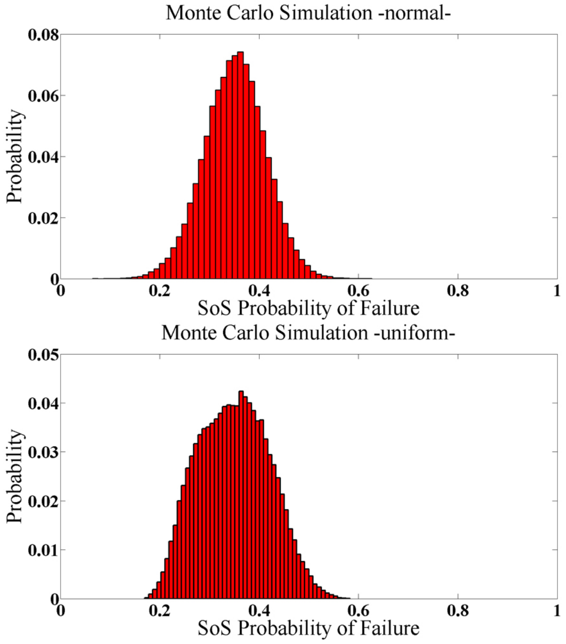


Fig. 12. Sensitivity analysis of SoS with Monte Carlo simulation at 10 000 h of operation using BN. (a) Normal. (b) Uniform distribution.

C. Dynamic and Emergent Behavior of the Proposed Framework

In the previous subsections, the hybrid HAZOP-FTA method along with the BN modeling and the sensitivity analysis was implemented to evaluate the impact of unknown events, such as the addition of new systems which is a part of the evolution of the SoS. In order to further study the emergent behavior of the SoS under investigation, one should resort to techniques dealing with large degrees of uncertainty (deep uncertainty). Under conditions of deep uncertainty, it is hard to forecast the realizations and the time-varying relationships of relevant factors in the SoS. Furthermore, these situations of uncertainty can be occurred in a system that has not yet existed. The latter case is examined in this subsection since new versions of the SoS can be obtained through the addition or deletion or replacement of systems or links. Unfortunately, in deep uncertainty the appropriate conceptual models to describe interactions among SoS variables as well as the probability distributions to represent uncertainty about key parameters in the models are unknown.

In order to calm down model assumptions that are necessary to address uncertainty, a series of computational experiments should be performed. The numerical simulations include evaluations of model outcomes across a large set of possible SoS representations. Each plausible SoS representation can be assumed as one hypothesis about SoS behavior. By investigating a large set of such hypotheses and by evaluating their correctness, the "whole picture" of SoS emergent behavior can be obtained.

A simple method for constructing the possible SoS models is to include time in the model specification defining the evolution of the SoS model. Without loss of generality, a discrete rather than continuous approach in modeling the time evolution is considered. The evolutionary modeling of SoS is depicted in Fig. 13.

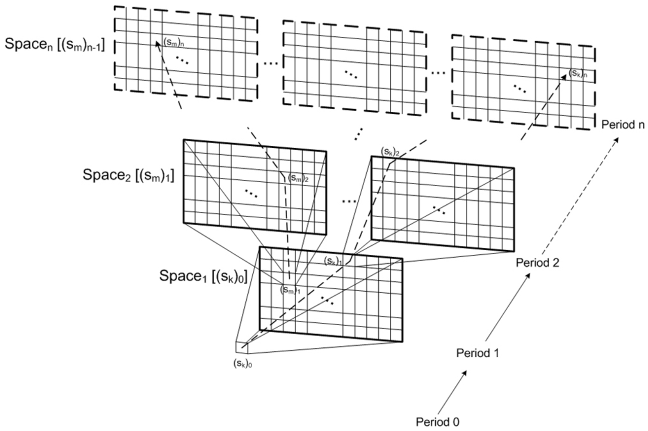


Fig. 13. Network realization along with uncertainty spaces.

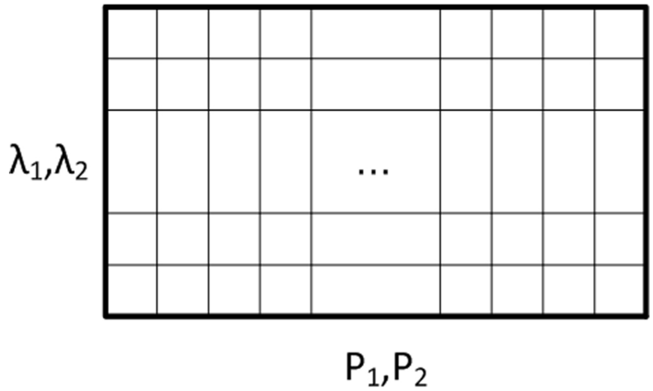


Fig. 14. SoS plausible representation for different combinations of failure rates and parallel systems probabilities of failure.

TABLE V

PARAMETERS OF THE REALIZATION

aa	λ_1	λ_2	P_1	P_2
1	80% $\lambda_{1,in}$	80% $\lambda_{2,\mathrm{in}}$	0.3	0.3
2	90% $\lambda_{1,\mathrm{in}}$	90% $\lambda_{2,\mathrm{in}}$	0.4	0.4
3	$\lambda_{1,\mathrm{in}=}0.000135$	$\lambda_{2,\mathrm{in}=}0.000312$	0.5	0.5
4	110% $\lambda_{1,\mathrm{in}}$	110% $\lambda_{2,\mathrm{in}}$	0.6	0.6
5	120% $\lambda_{1,\mathrm{in}}$	120% $\lambda_{2,\mathrm{in}}$	0.7	0.7

As shown in Fig. 13, there is a dependence of uncertainty spaces in a period i on the realizations of all the preceding periods. For example in Period 2, the uncertainty space (Space$_2$ [(s$_\mathrm{m}$)$_1$]) is generated from the realization (s$_\mathrm{m}$)$_1$ of the preceding uncertainty space (Space$_1$ [(s$_\mathrm{k}$)$_0$]), which in turn is originated from the initial condition (s$_\mathrm{k}$)$_0$. Hence, a possible future path (dashed lines) can be represented by the sequence $(\mathrm{s_k})_0 \rightarrow (\mathrm{s_k})_1 \rightarrow (\mathrm{s_k})_2 \ldots \rightarrow (\mathrm{s_k})_\mathrm{n}$.

In this paper, the time gap between two consequent periods is two years, while the parameters involved in each uncertainty space (Fig. 14) are the failure rates of the BRAS server and the CO switch as well as the probability of failure of the parallel to the CO and the LE systems. Each combination between the failure rates and the probability of failures of the parallel systems is a plausible SoS representation, while the path from the initial condition to this representation point describes the SoS behavior up to that period.

The values for the parameters λ_1, λ_2, P_1, P_2 are shown in Table V, where $\lambda_{\mathrm{i,in}}$ are the original values of the component's failure rate used in the previous sections.

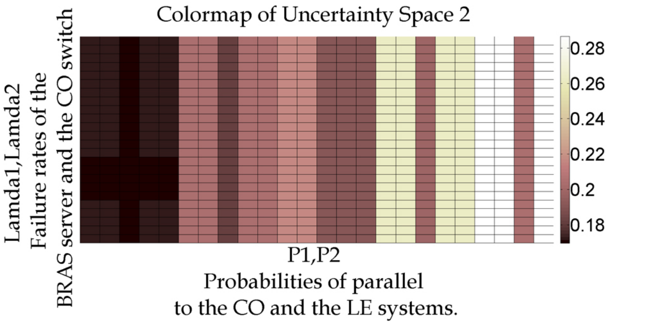


Fig. 15. One of the possible SoS representations after four years (period 2).

In Fig. 15, the uncertainty space 2 (after four years) originating from the realization (80% $\lambda_{1,in}$,110 % $\lambda_{2,in}$, 0.3, 0.5) of the previous period (2 years) is illustrated as a color map where different colors correspond to different probability values estimated using

$$P(SoS = True|CPE = False, DSLAM, LE, CO, BRASS) \tag{5}$$

$$= \frac{\sum_{D,L,CO,B[True,False]} P(SoS = T, C, = F, D, L, CO, B)}{\sum_{SOS,DL,CO,B\in[True,False]} P(SoS, C = F, D, L, CO, B)}.$$

In order to simplify Fig. 15 the coordinates of each realization are omitted. However, a method for determining the coordinates of a realization k (ith line and jth column of Fig. 15) is provided by the following equations:

$$\lambda_{1,k} = \lambda_1 \left(\left\lfloor \frac{i-1}{5} \right\rfloor + 1 \right) \tag{6a}$$

$$\lambda_{2,k} = \lambda_2\,(\mathrm{mod}\,((\mathrm{i}-1)\,, 5) + 1) \tag{6b}$$

$$P_{1,k} = P_1 \left(\left\lfloor \frac{j-1}{5} \right\rfloor + 1 \right) \tag{6c}$$

$$P_{2,k} = P_2\,(\mathrm{mod}\,((j-1)\,, 5) + 1) \tag{6d}$$

where $\lfloor \mathrm{x} \rfloor$ denotes the integer part of x and $\lambda_i(m)$, $P_i(m)$ represent the mth entries of λ_i and P_i, respectively, in Table V. Using the color map of Fig. 15, one can predict the impact of possible changes (components replacement and/or addition or deletion of links—systems) in the infrastructure by estimating the values of conditional probabilities and determine the emergent behaviors of the SoS by exploring the corresponding paths.

V. CONCLUSION

In this paper, a new SoS framework for the reliability assessment of telecommunication networks was proposed. This was based on a combination of hazard analysis techniques along with the BN model and sensitivity analysis. The proposed framework was implemented in the case of a fiber-to-the-curb VDSL network. The probabilities of failure of both the constituent systems and SoS were evaluated. Several importance metrics were also calculated showing the significance of all events contribution. The impact of both residual mishap risk and unknown events was estimated. The SoS evolution, i.e., SoS changes stemming from link or system addition or replacement, was investigated through exploratory modeling. The obtained results revealed the importance of the proposed tool regarding the proper and uninterrupted operation of SoS under investigation.

The proposed methodology can be used for evaluation of network performance and monitoring of service quality and service level agreements in a telecommunication network. It can also be exploited in technoeconomic studies in order to evaluate the cost of operation, administration, and maintenance.

References

[1] W. C. Hardy, *QoS: Measurement and Evaluation of Telecommunications Quality of Service*, 1st ed. West Sussex, U.K.: Wiley, 2001.

[2] W. A. Crossley, "System of systems: An introduction of Purdue university schools of engineering's signature area," presented at the Engineering Systems Symp., MIT Engineering Systems Division, Cambridge, 2004.

[3] M. Jamshidi, *System of Systems Engineering: Innovations for the 21st Century*. Hoboken, NJ: Wiley, 2009.

[4] M. W. Maier, "Architecting principles for systems-of-systems," *Syst. Eng.*, vol. 1, no. 4, pp. 267–284, 1998.

[5] J. Boardman and B. Sauser, "System of systems: The meaning of of," in *Proc. IEEE/SMC Int. Conf. Syst. Syst. Eng.*, Apr. 2006, p. 6.

[6] W. C. Baldwin and B. Sauser, "Modeling the characteristics of system of systems," in *Proc. IEEE Int. Conf. SoSE*, May–Jun. 2009, pp. 1–6.

[7] W. Liang, "Fuzzy information fusion based quantitative HAZOP analysis for gas compressor units," in *Proc. WRI Global Congr. Intell. Syst.*, May 2009, pp. 423–427.

[8] H. Jong-Gyu, J. Hyung-Jeong, and K. Dong-Hee, "Hazard analysis of train control system using HAZOP-KR methods," in *Proc. ICEMS*, Oct. 2010, pp. 1971–1975.

[9] S. Liu and Z. Han, "Reliability analysis of transformer based on FTA and Monte Carlo method," in *Proc. APPEEC*, 2009, pp. 1–3.

[10] M. Towhidnejad, D. R. Wallace, and A. M. Gallo, "Fault tree analysis for software design," in *Proc. 27th Annu. NASA Goddard/IEEE Softw. Eng. Workshop*, Dec. 2002, pp. 24–29.

[11] L. Zhou, G. Cai, J. Yang, and L. Jia, "Monte Carlo simulation based on FTA in reliability analysis of door system," in *Proc. 2nd ICCAE*, Feb. 2010, pp. 713–717.

[12] Y. Zhu, L. Huo, L. Zhang, and Y. Wang, "Bayesian network based time-sequence simulation for power system reliability assessment," in *Proc. 7th MICAI*, Oct. 2008, pp. 271–277.

[13] Q.-Y. Li, M.-C. Jiang, H.-F. Li, and M.-Y. Lu, "Software reliability qualitative evaluation method based on Bayesian networks," in *Proc. 2nd ICETC*, Jun. 2010, pp. V4-446–V4-451.

[14] J. B. Michael, M.-T. Shing, K. J. Cruickshank, and P. J. Redmond, "Hazard analysis and validation metrics framework for system of systems software safety," *IEEE Syst. J.*, vol. 4, no. 2, pp. 186–197, Jun. 2010.

[15] P. Redmond, "A system-of-systems interface hazard analysis technique," M.S. thesis, Naval Postgraduate School, Monterey, CA, 2007.

[16] V. R. Basili and H. D. Rombach, "The TAME project: Toward improvement-oriented software environments," *IEEE Trans. Softw. Eng.*, vol. 14, no. 6, pp. 758–773, Jun. 1988.

[17] X. H. C. Jiang, W. X. Li, J. Liu, and Z. Zhang, "A hybrid reliability approach based on probability and interval for uncertain structures," *ASME J. Mech. Des.*, vol. 134, p. 031001, Mar. 2012.

[18] X. Lu, H.-X. Li, and C. L. P. Chen, "Model-based probabilistic robust design with data-based uncertainty compensation for partially unknown system," *ASME J. Mech. Des.*, vol. 134, p. 021004, Feb. 2012.

[19] C. Weiwei, H. Ning, and K. Rui, "A reliability model with the dependent failures for telecommunication network," in *Proc. 8th ICRMS*, Jul. 2009, pp. 1129–1132.

[20] J. A. Abraham, "An improved algorithm for network reliability," *IEEE Trans. Reliab.*, vol. R-28, no. 1, pp. 58–61, Apr. 1979.

[21] O. R. Theologou and J. G. Carlier, "Factoring and reductions for networks with imperfect vertices," *IEEE Trans. Reliab.*, vol. 40, no. 2, pp. 210–217, Jun. 1991.

[22] P. K. Varshney, A. R. Joshi, and P.-L. Chang, "Reliability modeling and performance evaluation of variable link-capacity networks," *IEEE Trans. Reliab.*, vol. 43, no. 3, pp. 378–382, Sep. 1994.

[23] S. Sieteng and S. Rai, "An efficient cutset approach for evaluating communication-network reliability with heterogeneous link-capacities," *IEEE Trans. Reliab.*, vol. 54, no. 1, pp. 133–144, Mar. 2005.

[24] M. Hayashi and T. Abe, "Evaluating reliability of telecommunications networks using traffic path information," *IEEE Trans. Reliab.*, vol. 57, no. 2, pp. 283–294, Jun. 2008.

[25] L. Ruiying, H. Ning, and K. Rui, "Network failure characteristic analysis," in *Proc. 16th Int. Conf. Ind. Eng. Manage.*, Oct. 2009, pp. 1764–1768.

[26] P. J. Redmond, J. B. Michael, and P. V. Shebalin, "Interface hazard analysis for system of systems," in *Proc. IEEE Int. Conf. SoSE*, Jun. 2008, pp. 1–8.

[27] P. C. Pendharkar, "Maximum entropy and least square error minimizing procedures for estimating missing conditional probabilities in Bayesian networks," *Comput. Statist. Data Anal.*, vol. 52, no. 7, pp. 3583–3602, 2008.

[28] C. A. Ericson, *Hazard Analysis Techniques for System Safety*. Hoboken, NJ: Wiley, 2005.

[29] A. Darwiche, *Modeling and Reasoning With Bayesian Networks*. Cambridge, MA: Cambridge Univ. Press, 2009.

[30] IST-TONIC, EU. *IST-2000-25172* [Online]. Available: http://www-nrc.nokia.com/tonic/

[31] T. O. Walker, M. Tummala, and J. McEachen, "A system of systems study of space-based networks utilizing picosatellite formations," in *Proc. 5th Int. Conf. SoSE*, Jun. 2010, pp. 1–6.

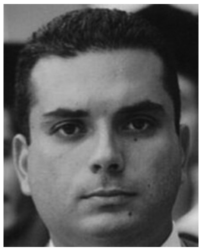
[32] I. Ahmad, J. Kamruzzaman, and D. Habibi, "Rerouting technique for faster restoration of preempted calls," in *Proc. 6th IEEE/ACIS ICIS*, Jul. 2007, pp. 676–681.

[33] R. Banner and A. Orda, "Designing low-capacity backup networks for fast restoration," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[34] D. Johnson, G. N. Brown, S. I. Beggs, C. P. Botham, I. Hawker, R. S. K. Chng, M. C. Sinclair, and M. J. O'Mahony, "Distributed restoration strategies in telecommunications networks," in *Proc. IEEE ICC and SUPERCOMM/ICC*, vol. 1. May 1994, pp. 483–488.

Kosmas Tsilipanos (M'03) was born in Athens, Greece, in 1976. He received the M.Sc. degree in radioelectrology and electronics from the University of Athens, Athens, where he is currently pursuing the Ph.D. degree.

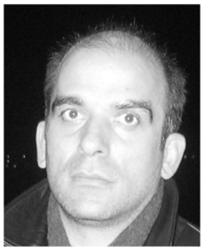
He is currently an Electronic Engineer with Broadcom Semiconductors. He has worked on various research projects with the National Center of Scientific Research "DEMOKRITOS," Athens. His current research interests include system of systems, network architectures and services, mobile communication systems, broadband and wireless systems, and evolutionary algorithms.



Ioannis Neokosmidis received the Physics degree, the M.Sc. degree in radioelectrology and electronics, and the Ph.D. diploma in optical nonlinear networks from the University of Athens, Athens, Greece.

He is currently a Research Associate with the University of Athens, and is an Adjunct Lecturer with Harokopion University, Athens. He has participated in European and national projects. He has 32 publications and more than 100 citations. His current research interests include system of systems, deep uncertainties, optical communications, and technoeconomics.

Dr. Neokosmidis serves as a reviewer for leading IEEE/OSA journals and conferences. He has received two Best Paper Awards. He is a biographee in several lists (*Marquis and Hübner's blaues Who's Who*).



Dimitris Varoutas (SM'11) received the Physics degree, and the M.Sc. and Ph.D. degrees in communications and technoeconomics from the University of Athens, Athens, Greece.

He is currently an Assistant Professor with the Department of Informatics and Telecommunications, University of Athens. He has published more than 100 publications in refereed journals and conferences in telecommunications, optoelectronics, and technoeconomics, including leading IEEE journals and conferences.

Dr. Varoutas is a Senior Member of the photonics (formerly LEOS), communications, education, and engineering management societies of IEEE, and serves as a reviewer in several journals and conferences, including those of IEEE. Since 2007, he has been a member of the BOG of ADAE, the National Authority for Communications Security and Privacy.