



# Dependability analysis and disaster recovery measures in smart hospital systems

Luiz Nelson Lima<sup>1</sup> · Arthur Sabino<sup>1</sup> · Vandırleya Barbosa<sup>1</sup> · Leonel Feitosa<sup>1</sup> · Carlos Brito<sup>1</sup> · Jean Araujo<sup>2</sup> · Francisco Airton Silva<sup>1</sup>

Received: 19 November 2023 / Accepted: 1 May 2024  
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2024

## Abstract

There is a growing importance of the Internet of Medical Things (IoMT), an emerging aspect of the Internet of Things (IoT), in smart healthcare. With the emergence of the Coronavirus (COVID-19) pandemic, healthcare systems faced extreme pressure, leading to the need for advancements and research focused on IoMT. Smart hospital infrastructures face challenges regarding availability and reliability measures, especially in the event of local server failures or disasters. Unpredictable malfunctions in any aspect of medical computing infrastructure, from the power system in a remote area to local computing systems in a smart hospital, can result in critical failures in medical monitoring services. These failures can have serious consequences, including potentially fatal loss of life in the most serious cases. Therefore, we propose a disaster analysis and recovery measures using Stochastic Petri Nets (SPN) to resolve these critical issues. The proposed model aims to identify the system's most critical components, develop strategies to mitigate failures and ensure system resilience. Our results show that the disaster recovery system demonstrated availability and reliability. The sensitivity analysis indicated the components that had the greatest impact on availability—for example, the failure time of the Standby Edge Server proved to be a very relevant component in the proposed architecture. The present work can help system architects develop distributed architectures considering points of failure and recovery measures.

**Keywords** Internet of Things · Smart hospital · Edge service · Disaster recovery · Reliability · Availability

## 1 Introduction

The Coronavirus (COVID-19) pandemic has triggered an unprecedented global crisis, putting healthcare systems worldwide under extreme pressure. Overloading on the wireless sensor networks (WSNs) used for medical monitoring and treatment has become a critical concern. The pandemic has accelerated research and development focused on this area due to the growing demand for reliable and sustainable medical services amid often uncertain failures in IoT infrastructures. The concept of IoT involves the use, processing, and storage of information in the cloud; such information is made available and can be used independently by intelligent objects connected to the cloud via the Internet [1, 7]. The pervasive development of the IoT and its use in medical research has improved the effectiveness of remote health monitoring systems [13, 14]. Healthcare systems are among these applications revolutionized with IoT, introducing a branch of IoT known as Internet-of-Medical Things (IoMT) systems, an

---

✉ Francisco Airton Silva  
faps@ufpi.edu.br

Luiz Nelson Lima  
luizznelson@ufpi.edu.br

Arthur Sabino  
arthursabino@ufpi.edu.br

Vandırleya Barbosa  
vandırleya.barbosa@ufpi.edu.br

Leonel Feitosa  
leonelfeitosa@ufpi.edu.br

Carlos Brito  
carlosvictor@ufpi.edu.br

Jean Araujo  
jean.araujo@fc.ul.pt

<sup>1</sup> Federal University of Piauí (UFPI), Picos, Piauí, Brazil

<sup>2</sup> Faculdade de Ciências, Universidade de Lisboa, Lisbon, Portugal

emerging area that is gaining researcher's attention due to its wide applicability in smart healthcare systems (SHS) [37].

Electrical infrastructure is critical in supporting the growing demand for IoMT-based healthcare systems. The reliable, uninterrupted operation of these systems depends on continuous power availability. Therefore, providing a sustainable and autonomous power supply is essential as it allows continuous power sensing, flexible positioning, reduced human intervention, and easy maintenance [6]. In smart hospitals, an electrical infrastructure must be designed with redundancy and stringent safety measures, ensuring that any interruption in power supply is quickly mitigated. Responsiveness is critical as a power infrastructure must support the constant operation of smart medical devices, local servers, and wireless sensor networks. Electricity distribution systems must be integrated with the corporate solutions of energy generators and distributors to guarantee greater reliability, availability, and agility in responding to emergencies [8]. "Adopting low-cost and energy-efficient strategies is essential to electrical infrastructure and meeting the critical needs of smart hospitals in the IoT era."

Elements of smart healthcare involve automated networks such as IoT, mobile Internet, cloud networking, big data, 5G, and artificial intelligence, along with evolving biotechnology [2]. Smart hospital infrastructure involves (i) wireless sensors for remote patient monitoring; (ii) IoT network devices (gateways, routers) used for data transmission; (iii) platform for data processing and analysis (cloud computing system, local servers) used for real-time analysis; (iv) smart medical devices (connected infusion pumps, smart vital signs monitors, IoT-connected diagnostic equipment) [34]. The constant operation of these services is extremely important to provide a more agile and effective response time arising from extreme situations. Service reliability allows doctors to respond to changes promptly, mainly because they rely on continuous information in real-time [30].

Hospital computing systems need to work as accurately and quickly as possible. However, more than a local server may be needed to handle a large volume of data on busy days. In this way, using cloud servers helps distribute data to be accessed remotely for treatments and diagnoses when the physical environment is challenging. Cloud computing has emerged as a vision of the utility computing paradigm that provides reliable and resilient infrastructure for users to store data remotely and use on-demand applications and services [36]. In the context of IoT, Edge Computing is a technology that enables reliable, context-aware, and low-latency services for various application areas such as smart healthcare, smart industry, and smart cities [12]. A local edge server presents crucial hospital monitoring and treatment conditions due to its faster response time for making relevant patient decisions. In the event of a local edge server failure, data can be lost, and decision response time can be significantly affected. The

existence of a local backup server to mitigate or even avoid problems like this is extremely important, as lives can be at risk.

IoMT creates an urgent need for transformation in traditional hospitals and medical centers. Failures in any part of the medical IT infrastructure, from the power system in remote areas to the local IT systems in a smart hospital, can lead to critical disruptions in medical monitoring services, resulting, in extreme cases, in fatal loss of life. Given this critical scenario, it is crucial that the initial design of medical computing infrastructure carefully considers the reliability and availability characteristics of the network in smart hospitals, especially under the possibility of uncertain failures in any part of the power resources or computing servers, including those arising from situational disasters. Reliability and availability are important indicators for evaluating the quality of a cloud provider's service. In this context, it is necessary to develop reliability and availability models that quantify the impact of disasters that may occur on the system's infrastructure. Creating different models, emphasizing the redundancy of computing resources and disaster recovery measures to increase availability in extreme cases, becomes essential to adapt the operations of smart hospitals to the pandemic context.

This work mainly focuses on analyzing dependability and implementing disaster recovery measures in intelligent systems in hospital environments. The analysis is based on Stochastic Petri Nets (SPN) to evaluate system availability and reliability considering hardware and software failures, disaster occurrence, and recovery. The proposed models aim to contribute pertinent information so that system designers can identify the system's most critical components and implement effective strategies and measures to mitigate failures and ensure system resilience. Faced with this problem, disaster recovery was implemented, considering a disaster on the edge server. The choice of this implementation demonstrated effectiveness in the proposal addressed, given the metrics analyzed. Our ultimate objective is to contribute to developing systems with more efficient disaster recovery measures regarding availability and reliability to face the challenges associated with this complex problem. The contributions of this paper are as follows:

- Two availability SPN models consider systems without and with disaster recovery measures to evaluate the availability of resources of a smart hospital. Availability is analyzed for both situations, indicating that adding disaster recovery is important.
- Two SPN models that calculate smart hospital reliability. The models are considered without and with disaster recovery measures. We vary a specific time, considering the increase in failure time of edge servers. The simulation was carried out considering both models, and the

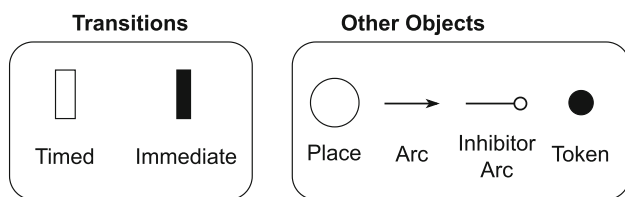


Fig. 1 SPN components

scenario with disaster recovery showed greater reliability.

- A sensitivity analysis with Design of Experiments (DoE) of the four proposed SPN models. The analysis demonstrated which components have the greatest impact on the availability of the entire system. The model considering disaster recovery on edge servers showed that edge server failure time has the greatest impact on availability. Thus, adding disaster recovery proved to be a valid strategy, as this component has a major impact on system availability in the recovery model.

The structure of this work is as follows: Sect. 2 presents the main concepts about Petri Nets and the DoE. Section 3 presents the main related works. Section 4 presents the system architecture that serves as the basis for our proposed SPN model, while Sect. 5 discusses the particularities of the proposed SPN models. The analytical results of a case study using the proposed models are presented in Sect. 6. Finally, Sect. 7 concludes the research and outlines future work.

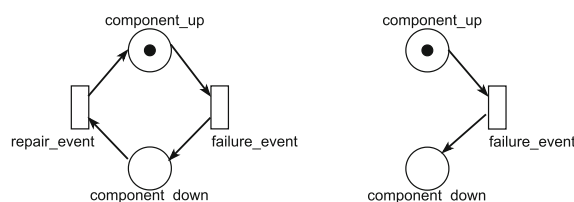
## 2 Background

In this section, we present the main essential concepts that will serve as the foundations for an in-depth understanding of the proposals explored throughout this work.

### 2.1 Stochastic petri net

Stochastic Petri Nets (SPNs) consist of two sections: the structural section, which defines the topology of the model with places, transitions, and connections, and the data (or parameters) section, which specifies stochastic information, such as transition rates and firing probabilities, to describe the probabilistic behavior of the system. Petri nets are tools used to analyze systems with concurrency and synchronization [18, 23, 24, 28]. SPNs can be identified as a directed graph divided into two parts, filled with three types of objects. These objects are places, transitions, and directed arcs that connect places to transitions and transitions to places [29]. Figure 1 shows the components that represent an SPN.

Transitions are classified according to the delay between enabling and triggering a transition; such a delay may be



(a) Generic availability SPN model. (b) Generic reliability SPN model.

Fig. 2 Example of an SPNs model to represent the availability and reliability of a generic component

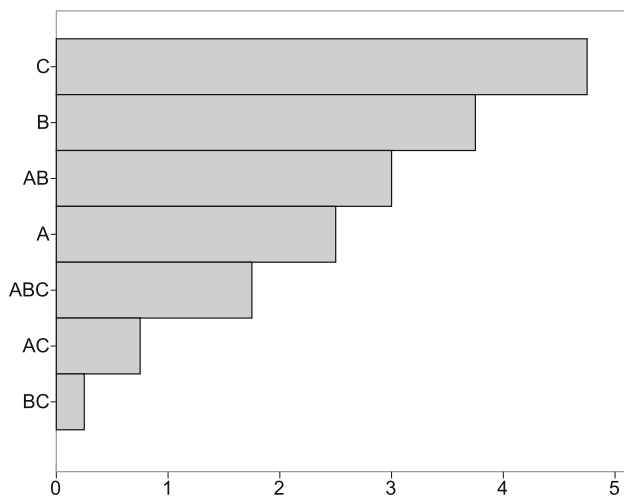
absent (an immediate transition), deterministic, or sampled from a given distribution (stochastic). When firing, a transition removes a token from its entry location and deposits it at its exit location [40]. On the other hand, immediate transitions are triggered instantly, without any waiting period. White circles symbolize the representation of places, and arrows symbolize arcs to establish connections between places and transitions. Inhibitory arcs are symbolized by a line with a small white ball at the end, where they can block or allow the flow of tokens from one place to another. A token symbolized by a small black ball is also assigned to a specific place. In SPN models that evaluate system availability and reliability, the concept of active and inactive components plays a crucial role. Figure 2 presents generic availability and reliability models that will be detailed below.

Figure 2a presents a generic example of an SPN model for availability. If there is a token in *component\_up*, it means the component is up. The component has entered a failed state if the *failure\_event* transition is enabled. A token is fired to the *component\_down* location, representing that the component is unavailable. This transition is modeled according to a stochastic process (generally followed by an exponential distribution) defined by the parameter (MTTF). The *repair\_event* transition represents repair, defined by the mean time to repair (MTTR). In this example, component availability is the probability of at least one token in *component\_up*.

Figure 2b presents a generic model for reliability. The difference with the availability model is the removal of the *repair\_event* component. The other components of the model follow the same flow. In this context, the reliability model aims to represent the system's or component's continuous functioning without considering the possibility of repairs or maintenance.

### 2.2 Sensitivity analysis with DoE

Sensitivity analysis systematically investigates the reaction of simulation responses to extreme values of the model input or drastic changes in the model structure [15]. It can also be defined by a series of tests where the researcher changes a set of variables or input factors to be observed and identifies the reasons for the changes in the output response [5]. The defi-



**Fig. 3** Generic example of factor effect graph

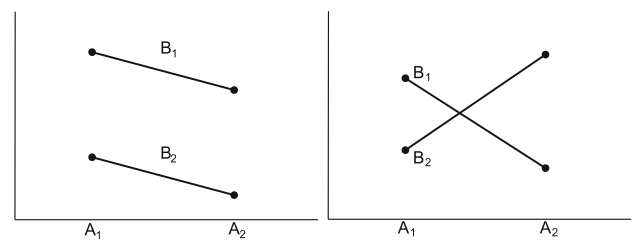
nition of the parameters to be modified is established through an experiment plan. The underlying objective is to obtain the maximum amount of meaningful information with as few experiments as possible. From these parameter variations, observing changes in the system's behavior through sets of outputs is possible. In specialized literature [9, 11, 33], we find three categories of graphs generally used in experiments with the DoE approach.

The factor effect graph, represented by bars arranged in descending order, highlights the relative impact of each factor. The higher the bar, the greater its impact, providing a clear view of the influences of each factor. Figure 3 presents an example of a factors effect graph. The graph shows three factors: A, B, and C. Factor C has the greatest impact.

Main effects plots play an important role in analyzing changes in the average levels of one or more factors. They visually present the average response for each factor level, connecting these points using lines. This chart type is especially valuable for comparing the relative impact of different factors. The sign and magnitude of the main effect point are, respectively, the average response value and the effect's intensity. A steeper slope of the line reflects a greater magnitude of the main effect, while a horizontal line indicates the absence of a main effect; this means that each factor level affects the response similarly. The interaction between factors A and B can be calculated using the Eq. 1.  $E_{A,B(+1)}$  refers to the effect of factor A when factor B is set at a high level. On the other hand,  $E_{A,B(-1)}$  indicates the effect of factor A when factor B is at a low level.

$$I_{A,B} = \frac{1}{2} (E_{A,B(+1)} - E_{A,B(-1)}) \quad (1)$$

Interaction graphs are intended to identify interactions between factors. An interaction occurs when the influence of a given factor on the outcome is changed (amplified or



(a) Low interaction between factors (b) High interaction between factors

**Fig. 4** Interaction graphs—examples with interaction and without interaction

reduced) by variation in the levels of another factor. If the lines on the graph are parallel, this indicates the absence of interaction between the factors. On the other hand, if the lines are not parallel, it is a sign of a significant interaction between the factors in question. Figure 4a represents an example where there are no interactions between the factors, as the lines are parallel. Figure 4b exemplifies a case of interaction between factors as the lines intersect. In this case, the change under a given metric for factor A at level A1 is higher than level A2. Changes in levels of factor A for some given metric indicate a dependence of factor A on the levels of factor B.

### 3 Related works

This section presents a literature review relating to the context of the proposed work. The papers were selected considering six selection criteria: context, system specification, type of model, assessing availability and reliability, and finally, energy-related components. The detailed description of papers is based on the classification of papers. The works were classified into two main groups based on the context. The study context is relevant when considering which smart hospital sector the literature is most situated in. Table 1 shows some important contributions of works related to this study, followed by their selection criteria.

#### 3.1 Smart hospital system

The first classification is described according to the works that present the Smart Hospital System context. Rodrigues et al. [30] emphasizes the need for quick response times and constant availability in smart hospitals. It suggests using Stochastic Petri Nets for performance and availability assessment of these systems, which could enhance healthcare and operational efficiency. Andrade et al. [3] proposes a model based on Petri Nets to evaluate the reliability of disaster recovery solutions in critical IoT (Internet of Things) infrastructures. This model aims to help ensure the availability and resilience of these infrastructures in adverse situations, pro-

**Table 1** Related works

| Work                   | Context               | System specification | Type of model | Availability | Reliability | Energy system |
|------------------------|-----------------------|----------------------|---------------|--------------|-------------|---------------|
| Rodrigues et al. [30]  | Smart hospital system | Edge/Cloud           | SPN           | ✓            | ✓           | ×             |
| Santos et al. [31]     | IoT healthcare system | Fog/Cloud            | SPN, RBD      | ✓            | ×           | ×             |
| Santos et al. [32]     | IoT healthcare system | Fog/Cloud            | SPN, RBD      | ✓            | ×           | ×             |
| Sadok et al. [10]      | IoT healthcare system | Edge/Fog/Cloud       | SPN, RBD      | ✓            | ×           | ×             |
| Andrade et al. [3]     | Smart hospital system | Edge/Cloud           | SPN, RBD      | ✓            | ×           | ×             |
| Nguyen et al. [21]     | Smart hospital system | Fog/Cloud            | FT, CTMC      | ✓            | ✓           | ×             |
| Rahmani et al. [26]    | Smart hospital system | Edge                 | CMS           | ×            | ✓           | ✓             |
| Valentim et al. [39]   | IoT healthcare system | Fog/Cloud            | SPN           | ✓            | ×           | ×             |
| Strielkina et al. [38] | IoT healthcare system | Undefined            | CTMC          | ✓            | ×           | ×             |
| Nguyen et al. [20]     | Smart hospital system | Edge/Fog             | SPN           | ✓            | ×           | ×             |
| This Work              | Smart hospital system | Edge/Cloud           | SPN           | ✓            | ✓           | ✓             |

viding a systematic approach to their analysis. Nguyen et al. [21] proposes a methodology to quantify reliability and security in an Internet of Medical Things (IoMT) infrastructure with cloud/fog/edge (CFE) computing. It uses hierarchical models and considers failures, including cyber-attacks. Rahmani et al. [26] proposes a methodology to quantify reliability and security in an Internet of Medical Things (IoMT) infrastructure with cloud/fog/edge (CFE) computing. Analyzes five case studies and four operational scenarios to improve the design of real-world IoMT systems. Nguyen et al. [20] proposes a comprehensive model to evaluate the performability of medical information systems in local hospitals. The study highlights the importance of load balancing and fail-over techniques to improve the continuity and quality of medical services, especially in high-demand situations such as pandemics.

### 3.2 IoT healthcare system

The second classification is based on works that present the IoT Healthcare System context. The classification refers to works focusing on monitoring, not the system itself. Santos et al. [31] highlights the growing adoption of IoT in home healthcare and associated challenges such as security and performance. The work emphasizes the importance of healthcare system availability and presents an optimization approach to maximize availability within budgetary constraints. Santos et al. [32] addresses the use of technologies such as fog and edge computing in IoT to improve the availability of electronic health systems (e-health), highlighting the importance of availability in this context. It uses stochastic models and optimization algorithms to maximize system availability, considering budget constraints, and compares three optimization algorithms. Sadok et al. [10] explores how IoT can improve healthcare systems with sensors and cloud and fog infrastructure for health monitoring. Stochastic models analyze the impact of failures on system availability,

emphasizing sensors and fog devices as critical components. Valentim et al. [39] discusses the increasing investments in IoT-enabled smart healthcare and the importance of system availability. It introduces a Generalized Stochastic Petri Net model to assess the availability of private cloud-based Medical IoT architecture. Strielkina et al. [38] addresses the emergence of the Internet of Medical Things (IoMT) for health monitoring, addressing the risks of device and infrastructure failures. It proposes using Markov models to consider security issues and includes a case study on attacks on vulnerabilities in the IoT healthcare system.

### 3.3 Contributions of this work

The objective of this work is to create SPN models to analyze the dependability metrics of a smart hospital system. The analysis is performed by modeling a smart hospital system. The analysis of dependability metrics brings advantages by offering clear understanding, precise identification of requirements, and detecting problems, for example. The factors mentioned help to model the system, facilitating planning, allowing the evaluation of alternatives, and reducing risks, resulting in more efficient and collaborative implementations. The proposed SPN model's evaluation considers system availability and reliability analysis. The model has two main versions. The first version is a model without disaster recovery, and the second version is a model considering disaster recovery. The analysis made it possible to prove that the system with disaster recovery has greater availability and reliability than the one without recovery. In addition, a sensitivity analysis was carried out with the DoE to verify how the system behaves with changes in some system components' resources. The analysis demonstrated that the system component that this study focused on applying disaster recovery is the component with the greatest impact on system availability. In this way, the model is made so that designers adjust the structure's parameters and number of components as needed.

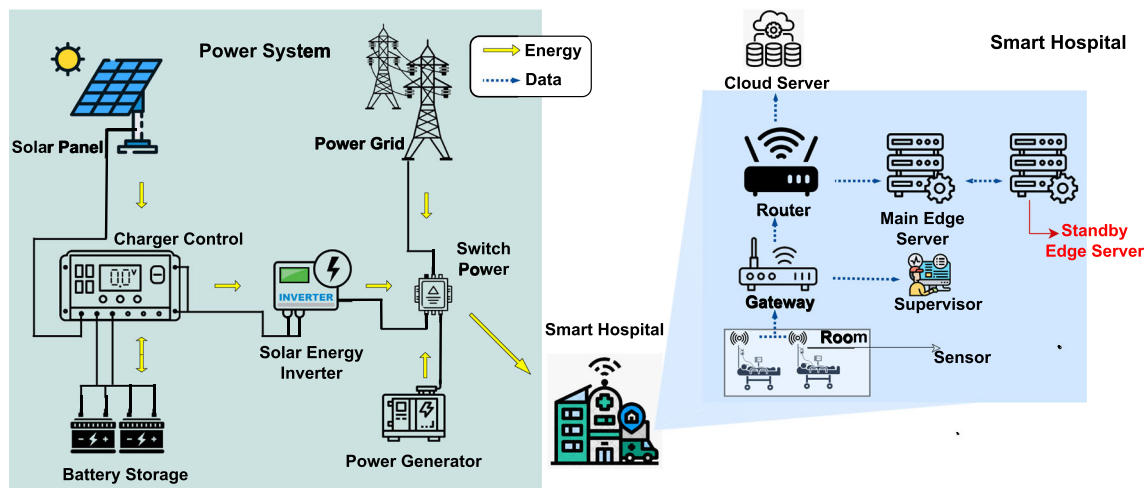


Fig. 5 System architecture

## 4 Architecture overview

This section describes the proposed architecture. Figure 5 presents the architecture used for this study. The architecture was divided into two main parts for better understanding. The first part on the left refers to the energy system that powers the hospital. The second part on the right is the smart hospital and its components.

The *power system* comprises three main energy sources: an *electrical grid*, a *power generator*, and a *solar power system* with solar panels. The *electrical grid* represents public energy supplied by public or private companies that do not have a direct connection with the hospital. The *power generator* runs on diesel, supplying power to the hospital during an outage. The *solar power system* comprises solar panels, charge controllers, battery storage, and solar power inverter; *battery storage* refers to batteries that store solar energy produced by solar panels. The batteries sustain the hospital's power for a short period until the main power resumes; the *charge controller* controls the energy from the panels stored in the batteries; the *solar energy inverter* can be understood as an electromagnetic energy converter where the conversion occurs from direct current (DC) to alternating current (AC) [27]; the *power switch* controls which power sources will be directed to the hospital. Given the overview of the energy components, the energy system works considering solar energy as the main feeder of the hospital. The electrical grid is used when solar energy fails. In the last case, the generator is activated when the other two energy resources fail.

The *smart hospital* is made up of components that distribute monitored information about patients. Rooms with sensors present in patient beds generate the monitored information. The information is forwarded to a gateway that distributes this data to the patient's supervisor and a router.

The supervisor is responsible for analyzing all data and taking action when necessary. The router transmits the data from the gateway to a server at the edge of the hospital and to a remote cloud server. The edge server will maintain data locally in the hospital to generate reports and queries and aid in decision-making. The hospital depends significantly on this data, so another edge server is built into the system—a standby (or partially powered on) server. The standby server is activated as soon as the hospital's main server experiences a failure, not due to a power outage. The server must be partially powered on to be activated more quickly when the main one is down. The remote cloud server stores data remotely as a backup for remote patient monitoring. For the hospital's components to function, the power must be working.

## 5 Proposed models

This section presents the proposed models following the architecture proposed in the previous section. The configurations followed for the models are based on the characteristics highlighted in the architecture. The proposed models help to evaluate the system's availability and reliability, considering disaster recovery and non-recovery scenarios. All models and simulations were performed using the Mercury Tool [16, 25]. The architecture modeling presented some limitations, therefore, we opted for some simplifications of the model. We did not investigate external factors that could affect the model's availability, such as user interaction, security risks, and climate change issues. The aforementioned specifications increase the complexity and size of the proposed architecture. We focus entirely on the local edge server failure process.

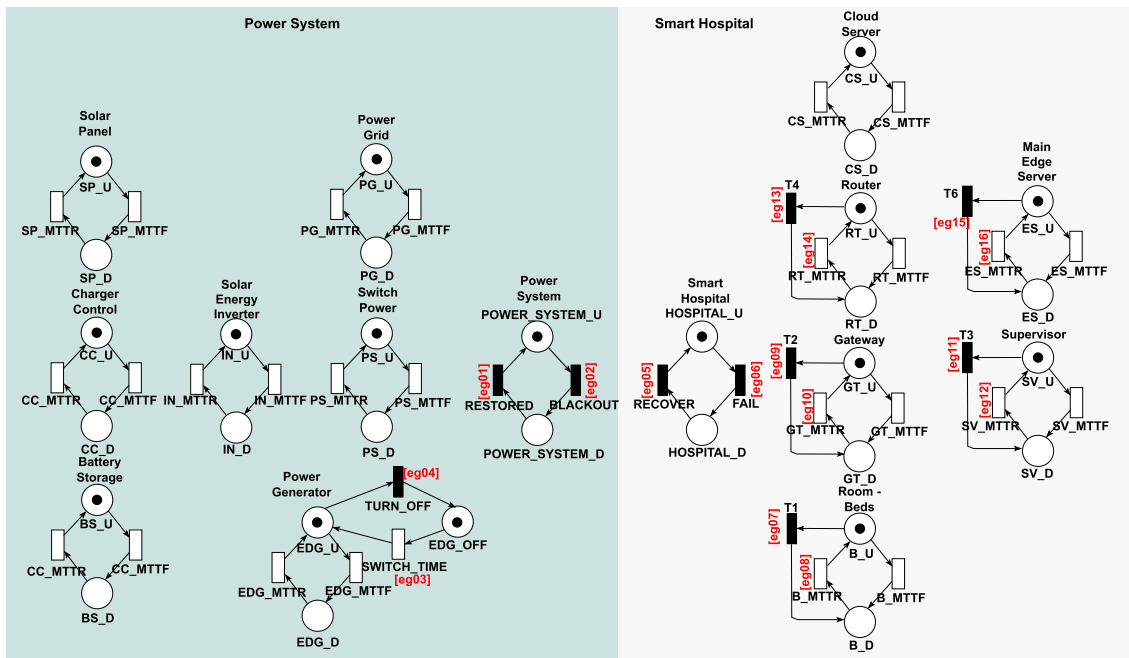


Fig. 6 Model without disaster recovery

### 5.1 Availability models

This subsection presents two models used to calculate systems availability: availability without disaster recovery and with disaster recovery.

#### 5.1.1 Model without disaster recovery

Figure 6 shows the availability model without disaster recovery. The hospital is operational if all of its internal components are active and if any power components are working. Two main components in the model control the states of the energy and hospital sectors: Power System and Smart Hospital. Control uses guard expressions in *RESTORED*, *BLACKOUT*, *RECOVER*, and *FAIL*. The two components used allow the system availability to be calculated. Model transitions that present text in red with e.g. followed by a number represent that the transition has a guard expression.

Table 2 presents the guard expressions for activation. A guard expression is a boolean expression that allows a transition to be enabled and can be fired. In addition to the current marking enabling this, the transition only becomes enabled and can be fired when the guard expression assigned to it is evaluated true [19].

The *Power System* component represents the system’s power state, whether active or inactive. *Power System* is considered active when there is a token in *POWER\_SYSTEM\_U* and inactive when there is a token in *POWER\_SYSTEM\_D*. State changes are controlled by *BLACKOUT* and *RESTORED* transitions. The mentioned transitions have guard expres-

sions. The *RESTORED* transition is activated when there is at least one active energy source, given by the expression *eg01*. The *BLACKOUT* transition is activated when all energy sources are unavailable and given by the expression *eg02*.

The *Smart Hospital* component denotes the status of the hospital. The hospital is considered active when all of its respective components are active. The inactive state occurs when any of the components have a token in the inactive state. The *Smart Hospital* is active when it has a token in *HOSPITAL\_U* and inactive when it is in *HOSPITAL\_D*. Controlling changes between active and inactive states occurs in *FAIL*, *RECOVER* transitions. The *FAIL* immediate transition is activated when all power components fail, indicating a power outage. The expression used in this transition is *eg06*. The *RECOVER* immediate transition is activated when at least one active power source powers the hospital. The guard expression used is *eg05*.

The *Power Generator* is a specific component for the power sector of the system. The behavior of the generator differs from the other components of the system. The use of the generator depends on a specific condition. The *SWITCH\_TIME* transition ensures that the energy generator enters the state of use only when there is no longer any energy source. The guard expression is given by *eg03*. The *TURN\_OFF* immediate transition ensures that this component is turned off immediately as soon as some other power component is active again. The expression for this is given by *eg04*.

**Table 2** Guard expressions for model

| Expression index             | Guard expression  |
|------------------------------|---|
| eg01                         | ((PS_U>0)AND(IN_U>0)AND(CC_U>0)AND((SP_U>0)OR(BS_U>0)))<br>OR(PG_U>0)OR(EDG_U>0)          |
| eg02                         | ((PS_U<1)OR(IN_U<1)OR(CC_U<1)OR((SP_U<1)AND<br>(BS_U<1)))AND(PG_U<1)AND(EDG_U<1)          |
| eg03                         | ((PS_U<1)OR(IN_U<1)OR(CC_U<1)OR((SP_U<1)AND(BS_U<1))) AND(PG_U<1)                         |
| eg04                         | ((PS_U>0)AND(IN_U>0)AND(CC_U>0)AND((SP_U>0)OR(BS_U>0))) OR<br>(PG_U>0)                    |
| eg05                         | ((CS_U>0)AND(ES_U>0)AND(RT_U>0)AND(GT_U>0)AND(B_D=0)<br>AND(SV_U>0))AND(POWER_SYSTEM_U>0) |
| eg06                         | (CS_U<1)OR(ES_U<1)OR(RT_D>0)OR(GT_D>0)OR(B_D>0)OR(SV_D>0)                                 |
| eg07, eg09, eg11, eg13, eg15 | (POWER_SYSTEM_D>0)  |
| eg08, eg10, eg12, eg14, eg16 | (POWER_SYSTEM_U>0)  |

The operation of the energy components follows the flow previously explained in Sect. 5. The *Solar Panel* generates energy by receiving sunlight; the *Charge Controller* adjusts the level of charge sent to the batteries and solar inverter; the *Batteries* stores energy that sustains the solar panel and ultimately can be used to power the hospital for a short period; the *Solar Inverter* converts solar energy for the hospital; *Switch Power* chooses which power source to take over when one of the sources fails; and finally, the *Power Generator* is only activated if all power sources fail.

The components of the hospital follow the characteristics already mentioned above. Sensors in patient rooms collect vital data about patients in beds; patient information is distributed to the supervisor and edge and cloud servers. Smart Hospital components have immediate transitions represented by *T1*, *T2*, *T3*, *T4*, *T6*. Transitions guarantee immediate failure of the hospital's components if the power supply fails and a blackout occurs. The expressions used for these elements are *eg07*, *eg09*, *eg11*, *eg13*, *eg15*. The timed transitions denoted in the components with *MTTF* indicate an average time when a system component can fail naturally. Timed transitions denoted with *MTTR* indicate the average recovery time for a component if it is inactive. Model components only recover their activity state if the Power System is active. The times manipulated in these components are crucial for analyzing the system's overall availability.

The main components, *Power System* and *Smart Hospital*, control the activity status of both system sectors. The components help to calculate the availability metric. Availability is calculated based on the probability that the *Power System* and the *Smart Hospital* run simultaneously. Equation 2 is used to calculate availability (A).

$$A = P((\#POWER\_SYSTEM\_U > 0)AND(\#HOSPITAL\_U > 0)) \quad (2)$$

*P* represents the probability, and (#) indicates the number of tokens in a given model element.

When evaluating system availability, it is also important to calculate Downtime (D). Downtime can be obtained by Eq. 3.

$$D = (1 - A) \times 8766 \quad (3)$$

*A* is the system availability and, 8766 is the number of hours present in a year.

### 5.1.2 Model with disaster recovery

Figure 7 shows the elements added to include disaster recovery. Disaster recovery is used for the edge server; the component is added to Smart Hospital. To consider an edge server failure that does not come from a power outage, an *ES\_D* element was added that indicates a server failure due to a disaster other than a power outage. When there is a token in *ES\_D*, it indicates a disaster-related downtime of the main edge server. The token in *ESR\_HOT* indicates that the backup server is on hot standby, that is, on standby or partially powered on. The token in *ESR\_HOT* can reach the used state in *ESR\_U* or idle state in *ESR\_D*. The downtime of the main server due to disaster activates the transition *TO\_ESD*, which has a guard condition for the token waiting to reach the state of use. The guard condition is represented by *eg18*. The backup server returns to standby mode if the main server returns to activity. As soon as the main server has the token in *ESD* fired to *ES\_U* again, the *RED\_ES* transition is fired. The mentioned transition indicates that the standby server that took over is redirected to the standby state again. The guard condition that activates the firing of *RED\_ES* is *eg19*. Finally, the backup server can reach an inactive state for two reasons. The first reason is the occurrence of a power outage. The immediate transition *T7* guarantees that the reserve



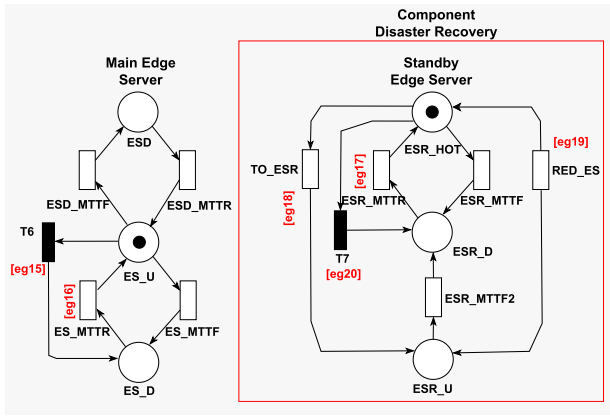


Fig. 7 Model with disaster recovery

Table 3 Guard expressions for model

| Expression index | Guard expression   |
|------------------|--------------------|
| eg18             | (ESD>0)            |
| eg17             | (POWER_SYSTEM_U>0) |
| eg19             | ((ES_U>0)          |
| eg20             | (POWER_SYSTEM_D>0) |

server changes its state to inactive, given by the guard condition *eg20*. The second reason occurs due to natural causes. Like the main one, the backup server can go down over time and become inactive. The backup server can go down while waiting or in a state of use. The transitions that indicate the time before the server can fail are represented by *ESR\_MTTF*, *ESR\_MTTR*, *ESR\_MTF2*.

Table 3 shows the guard conditions added to the previous model to consider disaster recovery on the edge server. The calculation of availability (A) and downtime (D) are made with the same equations mentioned previously. Availability is assessed considering elements added to the base model and downtime. Using the *Power System* and *Smart Hospital* core components helps maintain the same equation for the calculation.

### 5.2 Reliability model

Reliability is the conditional probability of a system remaining operational in a time interval [0, t], considering that it was operational at  $t = 0$  [34]. Figure 8 presents the reliability model. The model already includes the addition of the disaster recovery component, but the Standby Edge Server component is disregarded for the calculation. The operation of the model follows the same as that of availability. The difference with the availability model is that the components do not have elements that allow recovery from inactive to active

state. Removing these elements helps in calculating system reliability.

The reliability (R) of the mentioned models is calculated by Eq. 4, where P indicates the probability of the system being inactive in any sectors that represent it. The equation helps generate a graph showing how reliability decreases over time.

$$R = 1 - P\{(\#POWER\_SYSTEM\_D > 0) OR (\#HOSPITAL\_D > 0)\} \tag{4}$$

## 6 Results analysis

In this section, we will discuss the main results of the sensitivity analyses, highlighting the relevance of this information for implementing computing systems in the hospital environment, focusing on its most important infrastructure components, availability, and reliability of its system. Table 4 presents the parameters used to feed the proposed models. The values used were taken from some validated studies. The parameters were taken from [4, 17, 22, 30, 34].

### 6.1 DoE

In this work, we use the DoE technique to analyze the system’s sensitivity without disaster recovery and with disaster recovery. This methodological consistency is critical to ascertain which variable combinations exert the most significant impact on the system [35]. For this analysis, we run simulations with varying input factors to understand what causes changes in the output.

Figure 9 presents the factor effect graph, which shows the impact of factors on the analyzed measure through bars in descending order. The higher the bar, the greater the influence of the corresponding factor. This chart assists in pinpointing and ranking crucial system factors. Figures 10 and 11 present interaction graphs, which use lines to show how factors interact. If the lines are parallel, there is no interaction between the factors; however, if the lines are not, the factors interact.

In the experiment conducted for the system in question, we explored the layers of the architecture in the sensitivity analysis. However, we will only present the interacting factors, as the interaction is verified based on the impact of the combination of factors on the availability metric. The factors adopted for the study are (i) ES\_MTTF, (ii) PG\_MTTF, (iii) SV\_MTTF, (iv) B\_MTTF, and (v) SP\_MTTF. Each factor has two levels: low setting and high setting. Table 5 presents all factors and levels analyzed, while Table 6 shows all combinations between factors and their respective levels.

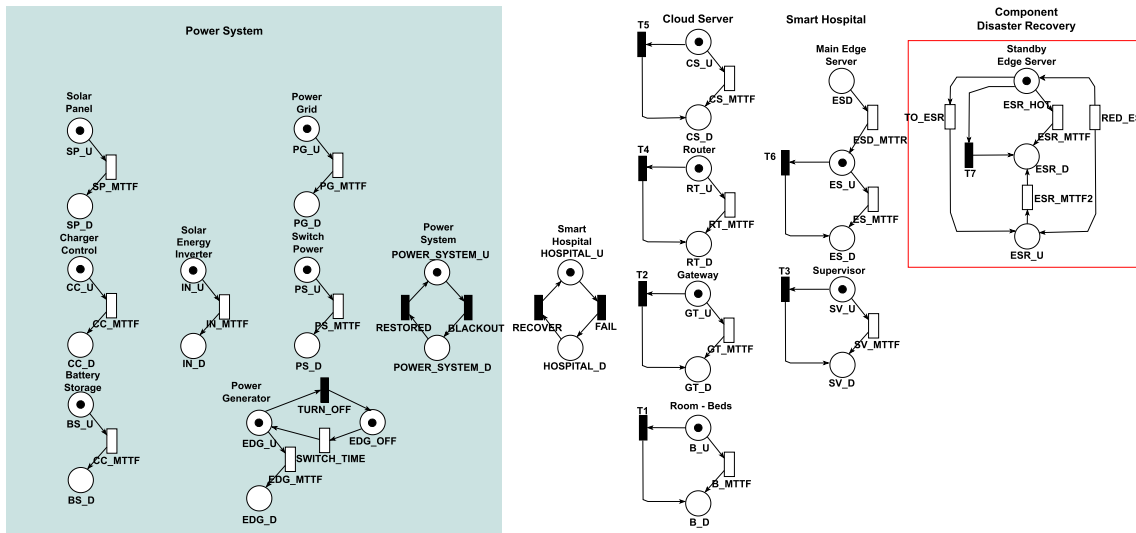
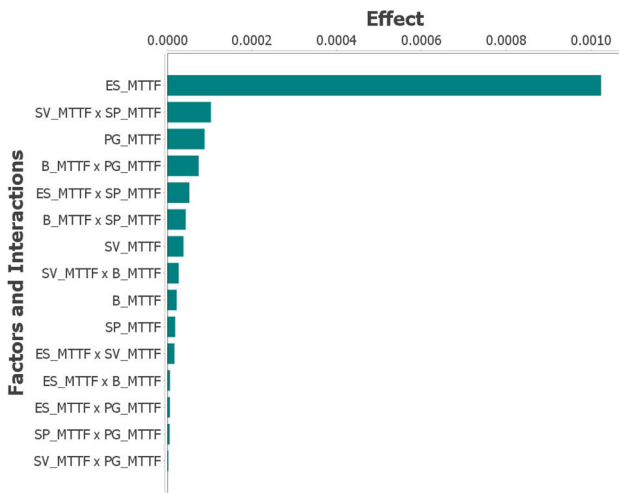
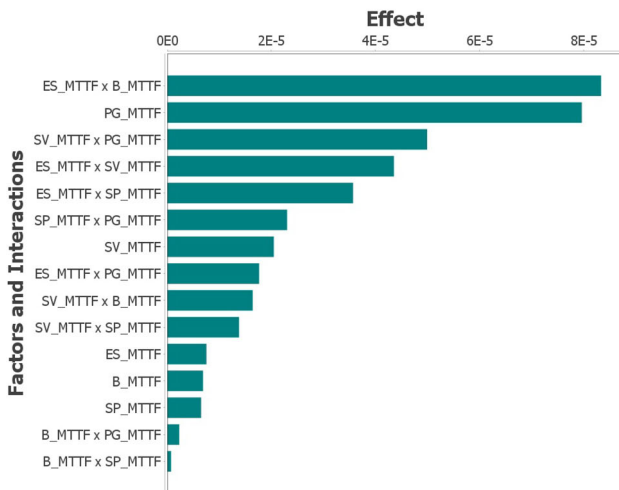


Fig. 8 Reliability model



(a) Impact of different factors on the system without disaster recovery



(b) Impact of different factors on the system with disaster recovery

Fig. 9 Impact of the factors of the two case studies

Table 4 Input parameters for proposed models

| Component             | MTTF (Hours) | MTTR (Hours) |
|-----------------------|--------------|--------------|
| Sensors/Actuators     | 300,000      | 1            |
| Gateway               | 480,770      | 8            |
| Supervisor            | 44,957       | 1            |
| Router                | 698,220      | 8            |
| Cloud server          | 760          | 0.74         |
| Edge servers          | 940          | 1.37         |
| Solar panel           | 219,000      | 8            |
| Battery storage       | 47,829       | 8            |
| Charge control        | 70,080       | 8            |
| Solar energy inverter | 24,820       | 8            |
| Power generator       | 636          | 37           |
| Power grid            | 8757         | 4.807        |

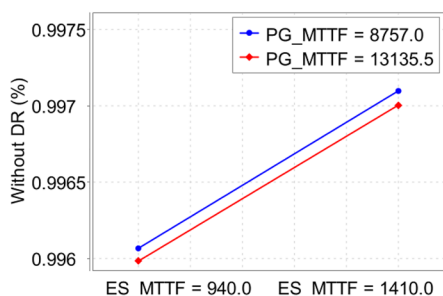
### 6.1.1 Without disaster recovery

Figure 9a displays the factor effect graph in the model without disaster recovery, which reveals the magnitude and importance of factors about the availability metric. This chart identifies factors that have a significant impact on simulations, leading to different values when their levels are altered.

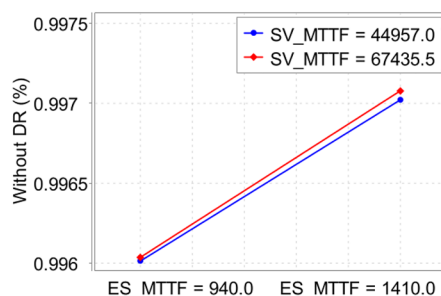
Among the factors analyzed, the time to failure of the edge server is the most relevant, which indicates that the time to failure is crucial for the system's efficiency. Furthermore, the time until power grid failure and the time until supervisor failure also play an important role in the context studied.

On the other hand, the time until sensors and solar panels fail has a smaller influence. Although it is a relevant factor, its impact on availability is relatively minor. The factor effect graph provides information about the absolute effects of fac-

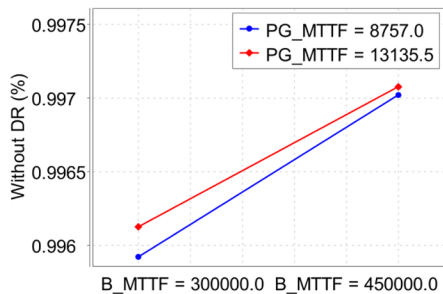
**Fig. 10** Interaction between factors and their impact on the system without disaster recovery



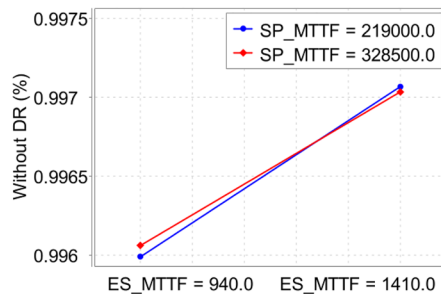
(a) Interaction between PG\_MTTF and ES\_MTTF



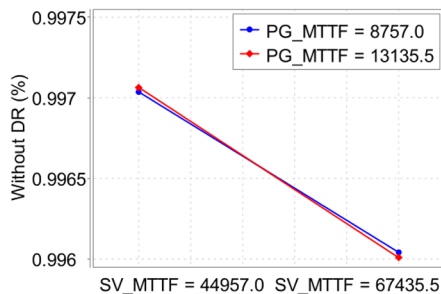
(b) Interaction between ES\_MTTF and SV\_MTTF



(c) Interaction between B\_MTTF and PG\_MTTF



(d) Interaction between ES\_MTTF and SP\_MTTF



(e) Interaction between SV\_MTTF and PG\_MTTF

tors, allowing one to determine which effects are significant but does not allow us to identify whether they increase or decrease availability.

Figure 10a shows the interaction between the factors *ES\_MTTF* and *PG\_MTTF*. It can be observed that these factors do not present any interaction with each other, maintaining a pattern of parallelism in all possible component failure time options. This means their variations do not influence each other regardless of the power grid failure time or the edge server failure time.

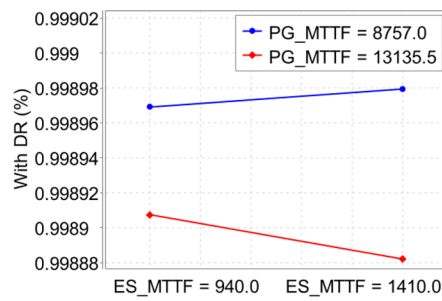
Figure 10b shows the interaction between the factors *ES\_MTTF* and *SV\_MTTF*. The supervisor’s times until failure shows similar movements, almost overwriting each other, but when it has a time until failure of 67435.5h, it always

presents better availability  $\approx 99,600$  to  $\approx 99,700\%$  regardless of the time until edge server failure.

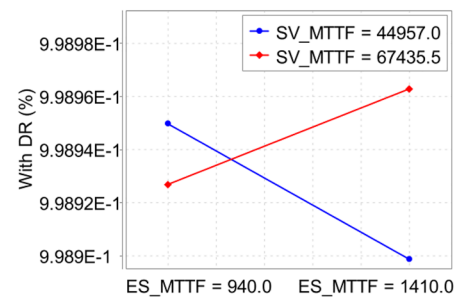
Figure 10c demonstrates the interaction between the factors *B\_MTTF* and *PG\_MTTF*. The times until failure of the power grid show similar movements, but when the time until failure is 13,135.5h, it always results in better availability, varying from  $\approx 99,600\%$  to  $\approx 99,700\%$ , regardless of the time until sensor failure.

Figure 10d shows the interaction between the factors *ES\_MTTF* and *SP\_MTTF*. The times to failure of solar panels exhibit similar movements. However, when the time to failure of the solar panels is 328,500h, it presents good availability with the edge server with a time to failure of 940h, but when the time to failure of the solar panels is 219,000h, it presents the best availability with the edge server with 1410h time to failure.

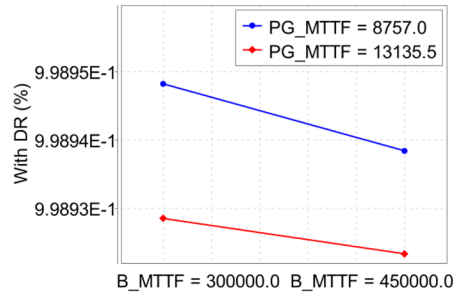
**Fig. 11** Interaction between factors and their impact on the system with disaster recovery



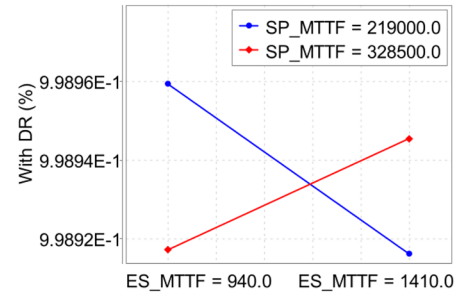
(a) Interaction between ES\_MTTF and PG\_MTTF



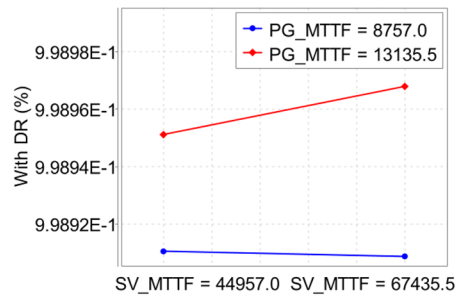
(b) Interaction between ES\_MTTF and SV\_MTTF



(c) Interaction between B\_MTTF and PG\_MTTF



(d) Interaction between ES\_MTTF and SP\_MTTF



(e) Interaction between SV\_MTTF and PG\_MTTF

**Table 5** Design table

| Factor name | Low setting | High setting |
|-------------|-------------|--------------|
| ES_MTTF     | 940.0       | 1410.0       |
| SV_MTTF     | 44,957.0    | 67,435.5     |
| B_MTTF      | 300,000.0   | 450,000.0    |
| SP_MTTF     | 219,000.0   | 328,500.0    |
| PG_MTTF     | 8757.0      | 131,35.5     |

Figure 10e shows the interaction between the factors *SV\_MTTF* and *PG\_MTTF*. Times until power grid failure exhibits similar movements. However, when the time to failure is 8757 h, good availability is obtained when the supervisor has a time to failure of 67435.5h. On the other hand, when the time until power grid failure is 8757 h, the best

availability is achieved when the supervisor has 44,957 h of time until failure.

### 6.1.2 With disaster recovery

Figure 9b presents the graph of factors' effect in the disaster recovery model, highlighting the difference in factors with the availability metric compared to the system without recovery. In this graph, we can see that with the recovery of the edge server, other factors underwent significant changes within the system.

The time until the power grid failure has become the most relevant factor in the system, indicating that the time until the power grid failure occurs is now the most impactful on the system. Furthermore, the time until failure of other factors such as the supervisor, sensors, and solar panels increased

**Table 6** Combination table

| ES_MTTF | SV_MTTF   | B_MTTF     | SP_MTTF    | PG_MTTF    | SRD & CRD |
|---------|-----------|------------|------------|------------|-----------|
| 940.00  | 44,957.00 | 300,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 940.00  | 44,957.00 | 300,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 940.00  | 44,957.00 | 300,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 940.00  | 44,957.00 | 300,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 940.00  | 44,957.00 | 450,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 940.00  | 44,957.00 | 450,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 940.00  | 44,957.00 | 450,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 940.00  | 44,957.00 | 450,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 940.00  | 67,435.50 | 300,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 940.00  | 67,435.50 | 300,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 940.00  | 67,435.50 | 300,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 940.00  | 67,435.50 | 300,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 940.00  | 67,435.50 | 450,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 940.00  | 67,435.50 | 450,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 940.00  | 67,435.50 | 450,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 940.00  | 67,435.50 | 450,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 1410.00 | 44,957.00 | 300,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 1410.00 | 44,957.00 | 300,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 1410.00 | 44,957.00 | 300,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 1410.00 | 44,957.00 | 300,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 1410.00 | 44,957.00 | 450,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 1410.00 | 44,957.00 | 450,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 1410.00 | 44,957.00 | 450,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 1410.00 | 44,957.00 | 450,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 1410.00 | 67,435.50 | 300,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 1410.00 | 67,435.50 | 300,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 1410.00 | 67,435.50 | 300,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 1410.00 | 67,435.50 | 300,000.00 | 328,500.00 | 13, 135.50 | 0.99      |
| 1410.00 | 67,435.50 | 450,000.00 | 219,000.00 | 8757.00    | 0.99      |
| 1410.00 | 67,435.50 | 450,000.00 | 219,000.00 | 13, 135.50 | 0.99      |
| 1410.00 | 67,435.50 | 450,000.00 | 328,500.00 | 8757.00    | 0.99      |
| 1410.00 | 67,435.50 | 450,000.00 | 328,500.00 | 13, 135.50 | 0.99      |

their importance in the system as a whole, but the time until failure of sensors and solar panels remained as the components that have less influence on the system availability.

Figure 11a shows the interaction between the factors *ES\_MTTF* and *PG\_MTTF*. Generally, the electrical grid with 8757 h of time until failure will always have better availability than with 13135.5 h of  $\approx 99.898\%$ . Considering 8757 h as the power grid failure time, the edge server failure time from 940 h to 1410 h is slightly increased. It may be that for an even higher value of the time until failure of the edge server. It could have an even higher result with the power grid with 8757 h.

Figure 11b shows the interaction between the factors *ES\_MTTF* and *SV\_MTTF*. The factors present a significant interaction. When using 940 h as the edge server failure time,

the best supervisor failure time is 44,957 h, resulting in an availability of  $\approx 99.895\%$ . The best availability is with the edge server failure time of 1410 h and the supervisor's failure time of 67,435.5 h, reaching  $\approx 99.896\%$  availability.

Figure 11c demonstrates the interaction between the factors *B\_MTTF* and *PG\_MTTF*. Generally, the power grid with 8757 h time to failure will always show better availability between  $\approx 99.894\%$  and  $99.895\%$  compared to 8757 h. Note that the best availability is with 8757 h as the power grid failure time and 300,000 h of sensors reaching  $\approx 99.895\%$  availability.

Figure 11d shows the interaction between the factors *ES\_MTTF* and *SP\_MTTF*. When the time to failure of the edge server is 940 h, the failure time of the good solar panels is 219,000 h, maximizing availability reaching up to  $\approx$

99,896%. When the edge server failure time is 1410h, the solar panel's failure time is 328,500h, and the maximum availability achieved is  $\approx 99,894\%$ .

Figure 11e displays the interaction between the factors *SV\_MTTF* and *PG\_MTTF*. Generally, the power grid with 13,135.5h time to failure will always have better availability of around  $\approx 99,897\%$  compared to 8757h. Looking at 13,135.5h as the mains failure time, we observe a slight increase in availability for a supervisor failure time between 44,957h and 67,435.5h. The result could be even higher with the power grid of 13,135.5h time to failure for an even higher value of the supervisor failure time.

## 6.2 Availability analysis

In this study, we employ approaches to analyze system availability to understand how the absence and application of disaster recovery measures affect its operability. Figure 12a displays the model's availability graph without disaster recovery, which reveals the relevance of the edge server about the availability metric. This chart shows how changes in the edge server's levels lead to significant differences in simulation outcomes, particularly in time-to-failure values.

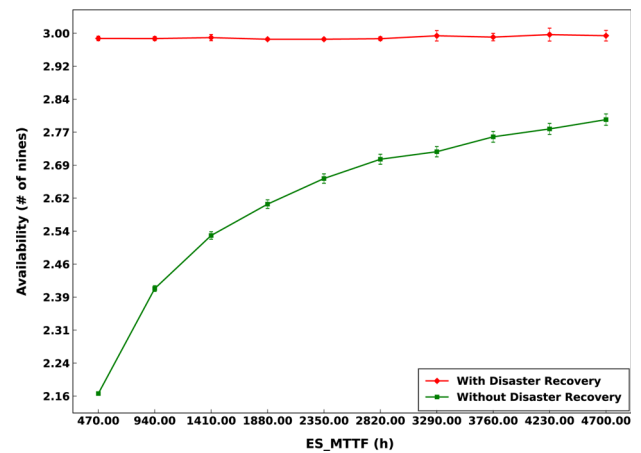
We can see in Fig. 12a that when the system does not have disaster recovery, system availability suffers significant impacts when the time until edge server failure is varied. Availability behaves so that the longer the time until the edge server fails, the greater the system availability.

The system with the inclusion of disaster recovery presents a completely different behavior. This is due to the lesser importance of the edge server as an isolated component. The system always presents greater availability when compared to the system without disaster recovery measures, remaining stable regardless of the time until the edge server fails.

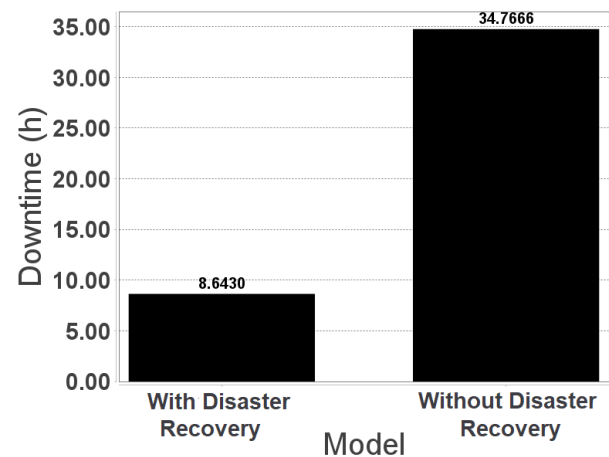
Figure 12b shows the downtime differences between the two systems, defined as periods when activities are halted or resources are inaccessible due to failures, maintenance, or interruptions. Edge server failure can lead to considerable system downtime without disaster recovery measures, resulting in  $\approx 35$ h. This significant interruption can have serious consequences for the proper functioning of the hospital service. When disaster recovery measures are implemented, downtime is significantly impacted, reducing compared to the system without recovery. The downtime shown with edge server disaster recovery measures is  $\approx 9$ h of downtime.

## 6.3 Reliability analysis

This study analyzes system reliability to see how strategies like disaster recovery affect the system's consistent, error-free performance. Figure 13 presents the reliability graphs of the models, in which we can notice the impact that the



(a) Comparison of case study availability



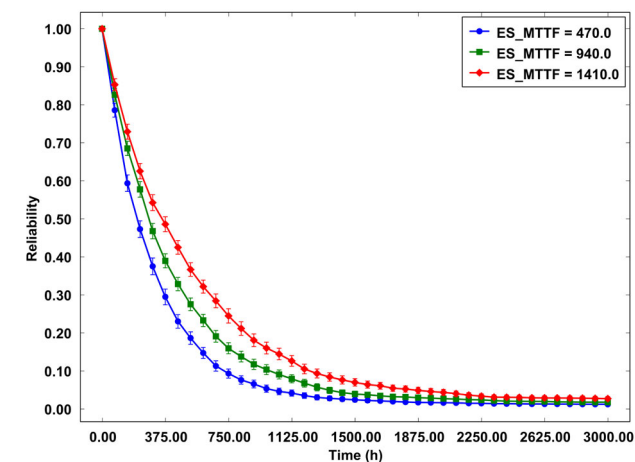
(b) Comparison of case study downtime

Fig. 12 Availability results of the two study cases

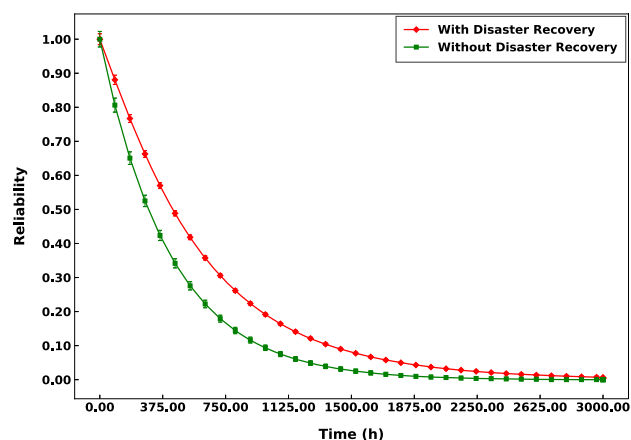
edge server time to failure values have on the reliability of the system, resulting in significantly different scenarios and the difference between the system without and with disaster recovery measures on the edge server.

Based on Fig. 13a, it is observed that in the absence of disaster recovery, system reliability is considerably affected by the variation in time until edge server failure. The trend evident is that the longer the time until edge server failure, the greater the system's overall reliability. This relationship between edge server lifetime and reliability is visible in the simulations, reflecting the strategic importance of ensuring the resilience and reliability of this critical system component.

Figure 13b shows the reliability of the two systems. The system without the presence of disaster recovery measures has lower reliability when compared to the system with disaster recovery measures. Due to the recovery measures, the system becomes more reliable, taking longer until it presents constant failures and has reduced reliability.



(a) Reliability Without Disaster Recovery



(b) Reliability Comparison

**Fig. 13** System reliability results with and without disaster recovery measures

## 6.4 Results discussion

The results provide valuable information for the design and management of smart hospital systems. Using SPN modeling, we evaluate the system's dependability, focusing mainly on the edge server. The analysis revealed that edge server failure time is a critical determinant of system efficiency. In practical terms, this underscores the need for system administrators to diligently maintain and monitor edge servers to maximize system availability. Furthermore, implementing a backup server can substantially increase availability, serving as an effective strategy to ensure uninterrupted services in a smart hospital.

However, it is crucial to recognize the limitations of the study: (i) To overcome the "state space explosion" issue, we had to simplify some models. For example, complex components such as the power grid and cloud servers were treated as encapsulated components with respective parameters Mean Time To Failure (MTTF) and Mean Time To Repair (MTTR);

(ii) Factors such as user interaction, security risks and environmental issues can sometimes impact availability. These aspects were not investigated in this study, which focused only on the failure process of local edge servers.

## 7 Conclusion

This study proposed Stochastic Petri Net (SPN) models to evaluate a smart hospital architecture, aiming to assist system administrators in planning computational architectures. The model considers several factors that influence the total availability of the system. The edge server is the main factor considered, and the use of a backup server showed a considerable increase in availability. Models provide accurate estimates of availability, downtime, and reliability metrics. The results show how each model behaves with varying parameters through sensitivity analyses. The analysis shows how the addition of a backup edge server strongly impacts the availability metric compared to the measurement without backup. In this sense, the case studies provide a practical guide that shows how a system administrator can apply the model to evaluate various configurations for a smart, consistent and sustainable hospital architecture. Future work intends to carry out a performance analysis to verify the impact that the availability of components can have on the response time and performance of the system. More external factors can also be considered, such as disasters in other components.

**Author Contributions** The authors contributed equally to this work.

**Funding** No funding was received for conducting this study.

**Data availability** Data sharing not applicable.

## Declarations

**Conflict of interest** The authors have no relevant financial or non-financial interests to disclose.

**Ethical approval** Not applicable.

## References

1. Abdulkareem KH, Mohammed MA, Salim A, Arif M, Geman O, Gupta D, Khanna A (2021) Realizing an effective covid-19 diagnosis system based on machine learning and iot in smart hospital environment. *IEEE Internet Things J* 8(21):15919–15928
2. Alshehri F, Muhammad G (2020) A comprehensive survey of the internet of things (iot) and ai-based smart healthcare. *IEEE Access* 9:3660–3678
3. Andrade E, Nogueira B (2020) Dependability evaluation of a disaster recovery solution for iot infrastructures. *J Supercomput* 76(3):1828–1849

4. Araujo E, Pereira P, Dantas J, Maciel P (2020) Dependability impact in the smart solar power systems: an analysis of smart buildings. *Energies* 14(1):124
5. Araújo G, Rodrigues L, Oliveira K, Fé I, Khan R, Silva FA (2021) Vehicular cloud computing networks: availability modelling and sensitivity analysis. *Int J Sensor Netw* 36(3):125–138
6. Ben Ammar M, Ben Dhaou I, El Houssaini D, Sahnoun S, Fakhfakh A, Kanoun O (2022) Requirements for energy-harvesting-driven edge devices using task-offloading approaches. *Electronics* 11(3):383
7. Bradley D, Russell D, Ferguson I, Isaacs J, MacLeod A, White R (2015) The internet of things-the future or the end of mechatronics. *Mechatronics* 27:57–74
8. Burian R, Gontijo M, Alvarez H (2019) Robustness and reliability in smart grid solutions. In: 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), pp 59–62
9. Costa I, Araujo J, Dantas J, Campos E, Silva FA, Maciel P (2016) Availability evaluation and sensitivity analysis of a mobile backend-as-a-service platform. *Qual Reliab Eng Int* 32(7):2191–2205
10. da Silva Lisboa MFF, Santos GL, Lynn T, Sadok D, Kelner J, Endo PT, et al (2018) Modeling the availability of an e-health system integrated with edge, fog and cloud infrastructures. In: 2018 IEEE symposium on computers and communications (ISCC), pp 00416–00421
11. Feitosa L, Gonçalves G, Nguyen TA, Lee JW, Silva FA (2021) Performance evaluation of message routing strategies in the internet of robotic things using the d/m/c/k/fcfs queuing network. *Electronics* 10(21):2626
12. Islam J, Kumar T, Kovacevic I, Harjula E (2021) Resource-aware dynamic service deployment for local iot edge computing: Healthcare use case. *IEEE Access* 9:115868–115884
13. Khan MA (2020) An iot framework for heart disease prediction based on mdnnc classifier. *IEEE Access* 8:34717–34727
14. Khan MA, Algarni F (2020) A healthcare monitoring system for the diagnosis of heart disease in the iomt cloud environment using msso-anfis. *IEEE Access* 8:122259–122269
15. Kleijnen JP (1995) Sensitivity analysis and optimization in simulation: design of experiments and case studies. In: Proceedings of the 27th conference on Winter simulation, pp 133–140
16. Maciel P, Matos R, Silva B, Figueiredo J, Oliveira D, Fé I, Maciel R, Dantas J (2017) Mercury: performance and dependability evaluation of systems with exponential, expolynomial, and general distributions. In: 2017 IEEE 22nd Pacific Rim international symposium on dependable computing (PRDC), pp 50–57
17. Marqusee J, Ericson S, Jenket D (2020) Emergency diesel generator reliability and installation energy security. Technical report, National Renewable Energy Lab.(NREL), Golden, CO (United States)
18. Marsan MA (1990) Stochastic petri nets: an elementary introduction. *Adv Petri Nets* 1989(9):1–29
19. MoDCS Research Group (2020) Mercury tool manual. In: CIn - Centro de Informatica UFPE, Recife, Brazil, March 13 2020. [Online] <http://www.modcs.org>
20. Nguyen TA, Fe I, Brito C, Kaliappan VK, Choi E, Min D, Lee JW, Silva FA (2021) Performability evaluation of load balancing and fail-over strategies for medical information systems with edge/fog computing using stochastic reward nets. *Sensors* 21(18):6253
21. Nguyen TA, Min D, Choi E, Lee J-W (2021) Dependability and security quantification of an internet of medical things infrastructure based on cloud-fog-edge continuum for healthcare monitoring using hierarchical models. *IEEE Internet Things J* 8(21):15704–15748
22. Perdue M, Gottschalg R (2015) Energy yields of small grid connected photovoltaic system: effects of component reliability and maintenance. *IET Renew Power Gener* 9(5):432–437
23. Peterson JL (1981) Petri net theory and the modeling of systems. Prentice Hall PTR
24. Petri CA (1962) Kommunikation mit automaten
25. Pinheiro T, Oliveira D, Matos R, Silva B, Pereira P, Melo C, Oliveira F, Tavares E, Dantas J, Maciel P (2021) The mercury environment: a modeling tool for performance and dependability evaluation. *Intelligent Environments* 2021
26. Rahmani AM, Hosseini Mirmahaleh SY (2022) Flexible-clustering based on application priority to improve iomt efficiency and dependability. *Sustainability* 14(17):10666
27. Rampinelli GA (2010) Study of electrical and thermal characteristics of inverters for grid-connected photovoltaic systems; estudo de características elétricas e térmicas de inversores para sistemas fotovoltaicos conectados a rede
28. Reisig W (1985) Petri nets. In: volume 4 of eates monographs in computer science
29. Rodrigues L, Gonçalves I, Fé I, Endo P, Silva FA (2020) Modelo estocástico para avaliação de disponibilidade de hospitais inteligentes. In: Anais do XIX Workshop em Desempenho de Sistemas Computacionais e de Comunicação, pp 145–156
30. Rodrigues L, Gonçalves I, Fé I, Endo PT, Silva FA (2021) Performance and availability evaluation of an smart hospital architecture. *Computing* 103:2401–2435
31. Santos GL, Gomes D, Kelner J, Sadok D, Silva FA, Endo PT, Lynn T (2020) The internet of things for healthcare: optimising e-health system availability in the fog and cloud. *Int J Comput Sci Eng* 21(4):615–628
32. Santos GL, Gomes D, Silva FA, Endo PT, Lynn T (2022) Maximising the availability of an internet of medical things system using surrogate models and nature-inspired approaches. *Int J Grid Util Comput* 13(2–3):291–308
33. Santos L, Cunha B, Fé I, Vieira M, Silva FA (2021) Data processing on edge and cloud: a performability evaluation and sensitivity analysis. *J Netw Syst Manag* 29(3):27
34. Silva FA, Brito C, Araújo G, Fé I, Tyan M, Lee J-W, Nguyen TA, Maciel PRM (2022) Model-driven impact quantification of energy resource redundancy and server rejuvenation on the dependability of medical sensor networks in smart hospitals. *Sensors* 22(4):1595
35. Silva LG, Cardoso I, Brito C, Barbosa V, Nogueira B, Choi E, Nguyen TA, Min D, Lee JW, Silva FA (2023) Urban advanced mobility dependability: a model-based quantification on vehicular ad hoc networks with virtual machine migration. *Sensors* 23(23):9485
36. Sookhak M, Gani A, Talebian H, Akhuzada A, Khan SU, Buyya R, Zomaya AY (2015) Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues. *ACM Comput Surv (CSUR)* 47(4):1–34
37. Srivastava J, Routray S, Ahmad S, Waris MM (2022) Internet of medical things (iomt)-based smart healthcare system: trends and progress. *Comput Intell Neurosci*
38. Strielkina A, Kharchenko V, Uzun D (2018) Availability models for healthcare iot systems: Classification and research considering attacks on vulnerabilities. In: 2018 IEEE 9th international conference on dependable systems, services and technologies (DESSERT), pp 58–62



39. Valentim T, Callou G, Vinicius A, França C, Tavares E (2023) Availability assessment of internet of medical things architecture using private cloud. In: Anais do L Seminário Integrado de Software e Hardware, pp 13–23
40. Volovoi V (2006) Stochastic petri nets modeling using spn@. In: RAMS'06. Annual Reliability and Maintainability Symposium, 2006, pp 75–81

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.