A Modeling-Based Approach for Dependability Analysis of a Constellation of Satellites

Daniel Farias[1†], Bruno Nogueira[2,3†], Ivaldir Farias Júnior[3†], Ermeson Andrade[1*†]

[1*]Departamento de Computação, Universidade Federal Rural de Pernambuco, Recife, Pernambuco, Brasil.
[2]Instituto de Computação, Universidade Federal de Pernambuco, Maceió, Alagoas, Brasil.
[3]Programa de Pós-Graduação em Engenharia da Computação, Universidade de Pernambuco, Recife, Pernambuco, Brasil.

*Corresponding author(s). E-mail(s): ermeson.andrade@ufrpe.br;
Contributing authors: daniel.farias@ufrpe.br; bruno@ic.ufal.br; ivaldir.farias@upe.br;
[†]These authors contributed equally to this work.

Abstract

Satellite constellations play critical roles across various sectors, encompassing communication, Earth observation, and space exploration. Ensuring the dependable operation of these constellations is of utmost importance. This paper introduces a dependability modeling approach using stochastic Petri nets to analyze satellite constellations. The primary focus is on improving operational efficiency through the assessment of availability, reliability, and maintainability. The approach helps satellite designers make informed decisions when selecting constellation configurations by assessing various dependability metrics. Using a global navigation satellite system as a case study, we conduct extensive numerical experiments to evaluate the feasibility of our approach. The results demonstrate quantitatively the significant impact of redundant components on both reliability and availability. They also illustrate how utilizing satellites in repair and operational orbits can influence these metrics and highlight the direct correlation between reliability and maintainability.

Keywords: Dependability, Constellation Dependability Approach, Satellite Constellations, Stochastic Petri Net.

1 Introduction

The rise of satellite constellations in recent years has guided in a new era of global infrastructure, impacting diverse fields like communication, Earth observation, and space exploration [1]. The vast coverage demands of these applications exceed the capabilities of a single satellite, necessitating collaboration among multiple satellites in a single orbital formation known as a constellation [2]. These constellations, comprising a network of interconnected satellites orbiting Earth, operate in harmony to achieve shared objectives. By exploiting the collective power of multiple satellites, these constellations enable global connectivity, facilitate seamless data transmission, and provide critical support to various industries [3]. However, ensuring the reliable and continuous operation of these constellations has become a central concern.

Malfunctions or interruptions in satellite constellations can have significant and widespread consequences. These disruptions can compromise connectivity for vital services such as emergency communications, global navigation systems, and weather forecasting [4–6]. Interruptions in satellite data transmission for Earth observation, for instance, can interfere with crucial environmental monitoring and disaster management efforts, significantly affecting our capability to predict and respond effectively to natural disasters. Therefore, ensuring the robust and uninterrupted operation of these satellite constellations is essential. This necessitates comprehensive dependability analyses and the implementation of strategies to mitigate risks associated with potential failures.

Dependability is a broad term encompassing reliability, availability, maintainability and other aspects such as safety, confidentiality and integrity, which collectively define the trustworthiness and consistency of a system or service [7, 8]. In the context of satellite constellations, the key attributes of reliability, availability, and maintainability are indispensable. Reliability ensures that satellites function consistently in specified configurations over time. Availability guarantees their accessibility to provide services when needed. Maintainability, on the other hand, allows for efficient repair, upgrades, or replacement of satellites, extending their lifespan and facilitating the continuous operation of the constellation. Therefore, evaluating reliability, availability, and maintainability of satellite constellations, and managing and assessing them effectively, directly impacts their overall performance, longevity, and efficiency.

Although the concept of satellite constellations is not new, there has been a notable upsurge in interest in recent years, driven by significant investments in projects such as Starlink and OneWeb [9, 10]. However, despite this increased attention, few studies have been proposed to evaluate their dependability. The study in [11] assesses satellite constellation dependability using the PRISM framework, a method relying on continuous-time Markov chains (CTMCs) for system analysis. While effective for system verification, using PRISM demands expertise and effort to build and expand models. Furthermore, handling large or intricate systems might encounter challenges due to complexities associated with CTMCs. In [6], the impact of satellite outages on air navigation continuity is investigated, yet aspects related to reliability and maintainability were not considered in this study. In broader terms, investigations in this field exhibit limitations. They often rely on restricted models, limiting their broader applicability. Furthermore, certain studies do not prioritize evaluating dependability, crucial for aerospace missions. Therefore, addressing these limitations by developing more accessible modeling techniques and investigating specific dependability challenges faced by these constellations becomes essential.

In this work, we introduce an approach, called Constellation Dependability Approach (CDA), that relies on Stochastic Petri Nets (SPNs) to model, analyze, and optimize satellite constellations. SPNs serve as effective tools to analyze these environments and estimate crucial dependability metrics. We present a case study applied to a global navigation satellite system to assess the feasibility and practicality of CDA. The obtained quantitative results distinctly demonstrate the significant impact of redundant components on the reliability and availability of constellations. Additionally, these findings illustrate how deploying satellites in repair and operational orbits can influence these metrics and emphasize the direct correlation between reliability and maintainability.

The contributions of this work are:

- Proposing dependable models suitable for satellite constellations. These models assist satellite designers in selecting configurations that aligns with mission requirements and budget constraints.
- Employing the SPN modeling approach to represent: (1) launch environment, (2) space and earth components, (3) orbit dynamics, and (4) diverse failure-recovery behaviors.
- Utilizing the SPN modeling technique to estimate crucial dependability metrics, such as service availability, probability of failures, the necessary number of satellites, among others.
- Presenting a case study where our modeling approach is applied to analyze a real-world satellite constellation.
- Demonstrating the adaptability of the proposed models, allowing for easy extension to represent various types of constellations.

The remainder of the paper is organized as follows: Section 2 introduces the related work in the field. Section 3 describes the proposed approach in detail. Section 4 elaborates on the specific global navigation satellite systems adopted for our analysis. Section 5 illustrates the proposed dependability models designed for the global navigation satellite systems. Section 6 details the dependability results obtained through numerical analysis. Section 7 concludes the paper and a brief discussion on future research directions.

2 Related work

Although the concept of satellite constellations predates the digital age, the recent surge in technology and the universal desire for internet connectivity everywhere have revived widespread interest in these satellite systems. Research in this field spans various areas. Detailed surveys on different aspects of satellite constellations, including constellation architecture, communication technologies, orbital dynamics, maintenance strategies, and more, can be found in [1, 12, 13]. However, these aspects require careful evaluation due to their expensive deployment and intricate operational requirements. To position our paper and highlight its contributions, we first summarize related studies focusing on the evaluation of different aspects of satellite constellations. Subsequently, we present studies that specifically assess particular aspects of the dependability of satellite constellations. Lastly, we compare our work to those used in these studies.

There is a vast amount of work analyzing various aspects of satellite constellations. In [14], Lee *et al.* present a simulation system for multipath mitigation in Global Navigation Satellite Systems (GNSS). The system uses spatial statistical methods to estimate signal multipath interference. The results of the evaluation show that multipath mitigation techniques based on spatial statistical methods are effective in reducing signal multipath interference. In the study by Shi *et al.* [15], they introduce a method using Petri nets to evaluate the robustness of satellite network defense systems against evolving cyber threats [15]. This method contributes to improving security and establishes a basis for resilience against more complex cyberattacks. By simulating and studying different attack possibilities, this research aims to strengthen satellite networks, reducing potential weaknesses. In addition to existing research, Polli *et al.* [16] propose an analytical model for assessing collision probabilities within large satellite constellations. This work anticipates and promotes enhanced space traffic management and operational safety. By precisely predicting potential collision scenarios, it enables proactive measures to ensure the sustainability and safety of satellite infrastructure.

There are also a few works that focus on certain aspects of the dependability of satellite constellations. In the study conducted by Zhai *et al.* [6], the impact of satellite outages on air navigation continuity is quantified. This research employs a simulation model to assess the effects of various outage scenarios. The simulation results reveal significant implications of satellite outages on air navigation. These outages have been found to potentially result in delays, flight cancellations, and even pose risks of accidents. In [17], the research proposes a comprehensive model integrating cost and coverage availability for optimizing satellite constellation systems. By focusing on economizing coverage while maintaining the required service quality, it addresses an important concern in satellite network deployment, ensuring optimized resource utilization.

In [18], the authors present an application of probabilistic model checking in analyzing the availability of satellite positioning systems for aviation, focusing on the use of the PRISM model checker. As PRISM is a formal method for specifying quantitative properties of a system model, it relies on for its analysis. Moreover, in a related publication [11], the authors expanded their earlier research [18] by incorporating considerations not only for availability but also for the reliability and maintainability of satellite positioning systems. Castet and Saleh [19] address the importance of reliability in space systems and investigated the reliability of satellite subsystems, aiming to identify the specific subsystems responsible for satellite failures. In [20], Hiriart *et al.* examine the comparative reliability of satellites in geosynchronous orbits (GEO), low Earth orbits (LEO), and medium Earth orbits (MEO).

Our work introduces a new approach from existing studies by presenting the CDA for modeling and analyzing satellite constellations. While prior research often relied on complex methods such as probabilistic model checking, which require intricate modeling techniques and can be challenging to interpret, the CDA utilizes SPNs. These SPNs offer a more intuitive and user-friendly approach for assessing dependability. Another limitation of previous studies is their reliance on restricted models like Markov chains, which are susceptible to state space explosion, and occasional omission of crucial dependability evaluations (ex.: reliability or maintainability). Our methodology addresses these gaps by proposing a comprehensive modeling, analysis, and optimization of dependability metrics in satellite constellations. This not only offers a more accessible alternative but also provides a practical solution for dependability assessment. Our objective is to provide satellite designers and operators with efficient tools adapted to their specific needs for assessing dependability. Additionally, the flexibility of SPN models facilitates easy expansion and application across different scenarios, enhancing their utility in addressing the diverse challenges encountered in satellite constellation operations.

3 Constellation Dependability Approach (CDA)

Assessing the dependability of satellite constellation systems is critical, particularly concerning reliability, availability, and maintainability aspects. Suppose we evaluate a satellite constellation to determine if it meets the required availability levels. How much could the overall availability improve by adding a redundant satellite? Can we achieve availability enhancements solely by including an extra satellite? Furthermore, how would the introduction of additional satellites affect the reliability of the satellite constellation environment, particularly when considering placing the redundant satellite in either the repair or operational orbit? Additionally, how many satellites would be required in a repair orbit to prevent the need for launching satellites from Earth within a designated time span? CDA aims to proactively address these questions to enhance the overall dependability of satellite constellation systems.

The proposed approach, presented in Figure 1, can start by selecting a specific satellite constellation system, such as GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), Galileo for global navigation, the Copernicus Sentinel constellation for Earth observation, Iridium NEXT for global voice and data coverage, the Cluster mission for studying Earth's magnetosphere, the Hubble Space Telescope for astrophysical observations, among others. Once the specific system is chosen, a comprehensive analysis of the selected satellite constellation, including its components and their interconnections, is conducted. It is worth mentioning that the constellation designers can use CDA to create a custom constellation from scratch, rather than selecting a preexisting system. Consequently, instead of choosing from predetermined constellations, designers can define the components and their interconnections as the first step of the approach.

Subsequently, we generate stochastic Petri net that represent both the chosen system and the desired dependability attributes, including availability, reliability, and maintainability. These models are utilized to compute key metrics, such as service availability, probability of failures, and the required number of satellites, enabling comprehensive dependability analyses. However, before conducting the analysis, it is

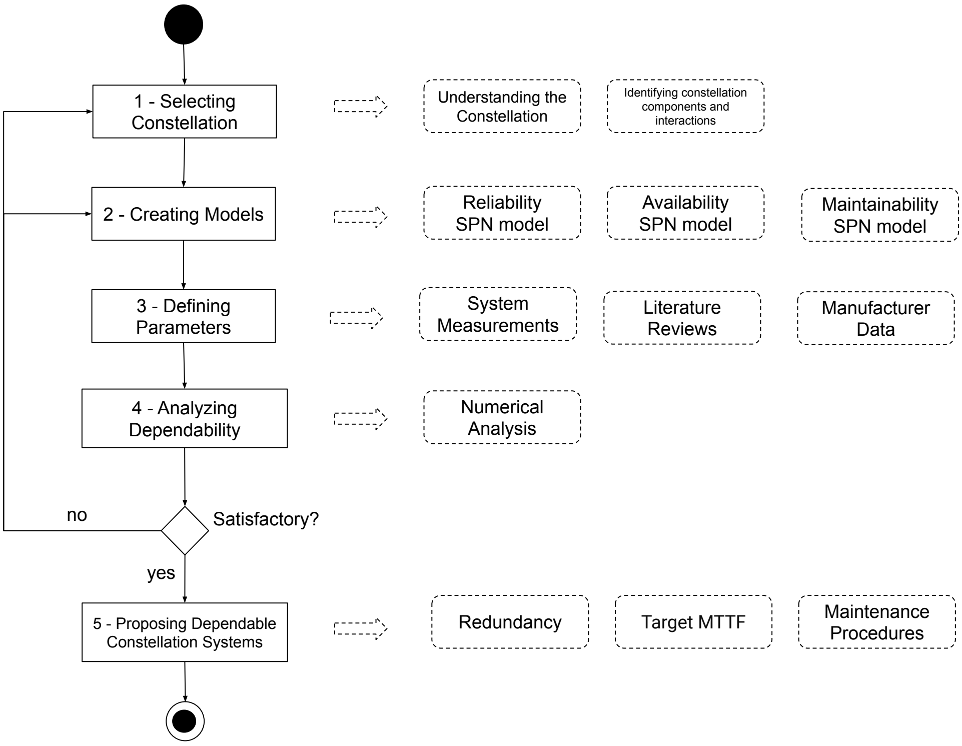


Fig. 1 Constellation dependability approach.

important to define the parameters of the models. These parameters can be derived from real system measurements, literature reviews, or manufacturer data. Once the parameters are established, the analysis can begin, which can be performed through either numerical analysis or simulation methods [21].

The analyses provide insight into the behavior of the satellite constellation system across diverse scenarios, considering environmental factors such as launch conditions, space and Earth components, and orbital dynamics. After achieving satisfactory model results that meet the dependability criteria and objectives of the constellation under analysis (i.e., ensuring a minimum service availability of 99% or minimizing the number of satellites requiring launch from Earth), CDA recommends dependable constellation systems. This may involve implementing redundancies strategies, setting target values for Mean Time To Failure (MTTF), and optimizing maintenance procedures. For example, if the objective is to enhance system availability, satisfactory model results would involve identifying constellation systems where the calculated availability meets or exceeds the specified target, such as achieving a minimum of 99% uptime. This allows designers to utilize these findings for constructing dependable systems that fulfill the specific mission requirements. If necessary, adjustments can be implemented, leading to a partial or complete re-execution of the approach. This iterative process ensures the accuracy and effectiveness of CDA in enhancing the overall dependability of satellite constellation systems.

4 Global Navigation Satellite Systems (GNSS)

To illustrate a practical application of the proposed CDA, we choose GNSS as a case study due to its widespread application and versatility [22]. However, our focus is not limited to any specific GNSS, as our objective is to apply our approach to study satellite constellations more broadly. A GNSS comprises three primary segments: the space segment, control segment, and user segment [23]. The space segment comprises multiple orbiting satellites transmitting positioning signals, while the control segment manages satellite orbits from ground-based stations. The user segment includes devices like smartphones and navigation systems, utilizing satellite signals for accurate positioning, navigation, and timing across diverse applications.

Figure 2 illustrates the implemented GNSS system based on [18]. Initially, monitor stations (MS) measure the distance to visible satellites and transmit this data to the master control station (MCS). The MCS collects, processes, and utilizes mathematical estimation methods to compute various parameters, such as navigation data, satellite orbit, timing parameters, among others. These results are then transmitted to ground antennas (GA) and subsequently sent to the satellites. Following this step, satellites transmit their current state data to users. Note that we considered two distinct orbital paths: an operational orbit, where active satellites provide services, and a dedicated repair orbit, where spare satellites are readily accessible for rapid deployment and replacement of any malfunctioning satellite in the operational orbit, minimizing service disruptions. Additionally, as mentioned by [14], it is critical to emphasize that users require information from at least four satellites to determine their position during navigation.

5 Dependability models

In this section, we first introduce Petri nets. Following that, the proposed models used to represent the GNSS system shown in Figure 2 are presented, aiming to compute metrics associated with availability, reliability, and maintainability.

5.1 Stochastic Petri nets

Petri nets are a family of formalism suited for modeling several system types due to their capability for representing concurrency, synchronization, communication mechanisms, and both deterministic and probabilistic delays. However, the original Petri net lacks the concept of time when analyzing performance and dependability. To address this, timed Petri nets were developed, which incorporate event durations. In this work, we employ the stochastic Petri net [24], a specific type of timed Petri net, where activity delays (represented by transitions) are modeled as random variables with an exponential distribution. Marsan *et al.* [25] proposed the Generalized Stochastic Petri Net (GSPN) as an extension of SPN, which considers two types of transitions: timed and immediate. Timed transitions have exponentially distributed firing times, while

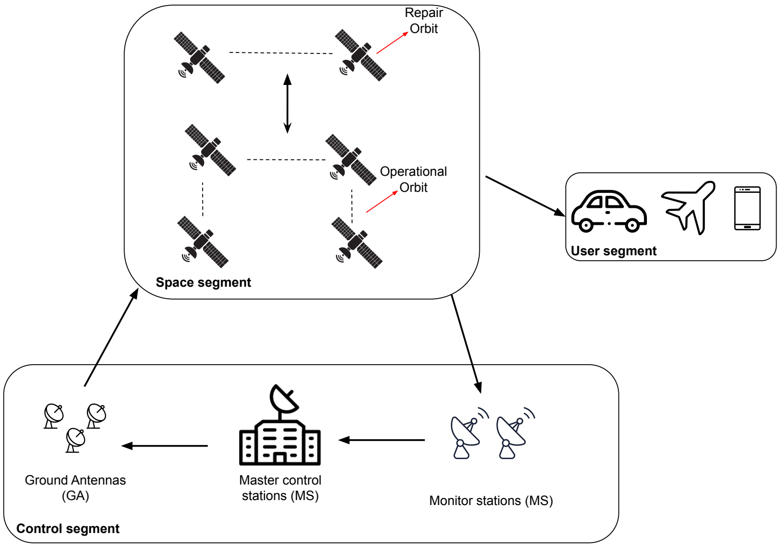


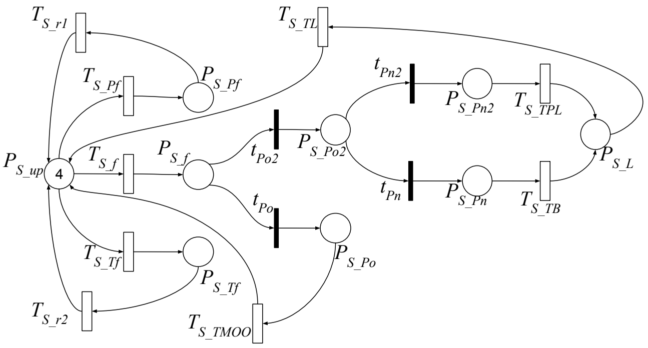
Fig. 2 Global navigation satellite systems

immediate transitions, by definition, fire instantly without any delay. For conciseness, we use the acronym SPN to refer to the entire family of models derived from the original stochastic Petri net defined in [24].

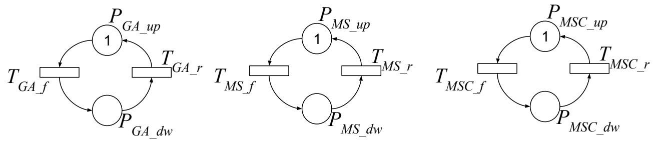
5.2 Availability models

Figure 3 shows the default availability models for the GNSS presented in Figure 2. The SPNs consist of interdependent sub-nets corresponding to a satellite, a GA, a MS and a MSC. The satellite model shown in Figure 3(a) represents the failure and recovery behaviour of a satellite. Initially, tokens are present in P_{S_up}, indicating that the satellites are in normal working condition. Note that the numerical value of "4" in P_{S_up} means that four satellites are active and operational. In this initial state, three types of interruptions can occur: planned, transient, and permanent. Planned interruptions occur when satellite maintenance is required, such as scheduled software updates, technical maintenance, or calibration procedures. For instance, scheduled software updates involve temporarily taking a satellite out of service to install new software versions for improved functionality or bug fixes. In such cases, the transition T_{S_Pf} is fired, leading to the removal of a token from P_{S_up} to P_{S_Pf}. Subsequently, transition T_{S_r1} becomes enabled, representing the completion of the planned repair. Upon the firing of T_{S_r1}, a token is removed from P_{S_Pf}, and a new token is deposited into P_{S_up}, meaning the satellite's return to the operational state after the planned maintenance.

Transient interruptions occur when satellite encounters temporary disturbances, such as minor signal interferences due to solar radiation, cosmic events, or passing through high-radiation zones in space. In such cases, the transition T_{S_Tf} is fired, resulting in the transfer of a token from P_{S_up} to P_{S_Tf}, indicating the satellite's



(a) Satellite Model



(b) Ground Antenna Model (c) Monitor Station Model (d) Master Control Station Model

Fig. 3 Constellation availability model.

transition from an operational state to a transient interruption state. Subsequently, transition T_{S_r2} becomes enabled, representing the completion or resolution of the transient interruption. Typically, transient interruptions are temporary and self-resolving, often disappearing automatically as the satellite moves out of the affected area or the interference diminishes. Upon the firing of T_{S_r2}, a token is removed from P_{S_Tf}, and a new token is placed into P_{S_up}, meaning the satellite's return to the operational state after the transient interruption has been resolved.

The last type of interruption is the permanent one, such as a critical hardware failure or an irreversible damage due to severe space debris collisions. Once such an event occurs, ground staff assess and decide upon the most effective repair strategy. It may involve the possibility of transferring a satellite from a repair orbit to its operational orbit, or alternatively, launching a new satellite from the ground to replace the damaged one. In such cases, the transition T_{S_f} moves a token from P_{S_up} to P_{S_f}, denoting the satellite's transition from operational to a state requiring replacement. Within this state, both transitions t_{Po} and t_{Po2} can be fired, where t_{Po} represents the probability of repairing the satellite while it remains in orbit, and t_{Po2} represents the probability of resolving the issue by launching a new satellite from the ground.

In scenarios where repairing the satellite while it remains in orbit is feasible, the transition t_{Po} is fired, transferring a token from P_{S_f} to P_{S_Po}, indicating that the satellite is prepared for replacement. Upon the firing of T_{S_TMOO}, a token is removed from P_{S_Po}, and a new token is placed into P_{S_up}, indicating the replacement of the satellite in the operational orbit by a spare satellite from the repair orbit. If repairing the satellite in orbit is not feasible, the transition t_{Po2} is fired, transferring a token from P_{S_f} to P_{S_Po2}, indicating the necessity of launching a new satellite. This launch can either involve using a satellite in a ready-to-launch state or require the creation of a new satellite. If a new satellite needs to be built, the transition t_{Pn} is fired, transferring a token from P_{S_Po2} to P_{S_Pn}, meaning the necessity of constructing a new satellite. Upon the firing of T_{S_TB}, a token is removed from P_{S_Pn}, and a new token is placed into P_{S_L}, indicating a new satellite is ready for launch. Alternatively, if a ready-to-launch satellite is available, a similar process occurs through the firing of transition t_{Pn2}. After that, both scenarios result in the launch of the satellite to the operational orbit by firing the transition T_{S_TL}, transferring a token from P_{S_L} to P_{S_up}.

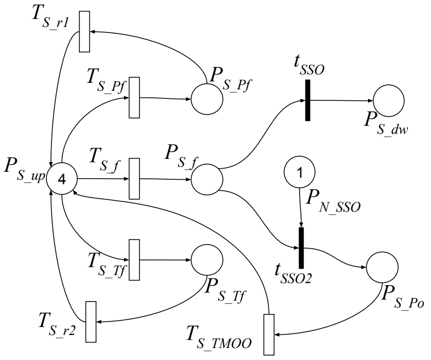
Figure 3(b) illustrates the SPN model for the ground antenna. This model, referred to as a basic model, depicts the failure and repair behavior of this component. In this model, a token placed in P_{GA_up} means the proper functioning of the antenna. Transitions T_{GA_f} and T_{GA_r} model the occurrence of failure and repair events, respectively. When transition T_{GA_f} is fired, a token is removed from the input place (P_{GA_up}), and a token is added to the output place (P_{GA_dw}), indicating the unavailability of the antenna. The antenna remains unavailable until transition T_{GA_r} is fired, which removes a token from place P_{GA_dw} and adds a token to place P_{GA_up}, representing the antenna's return to an available state. The redundancy of a component is reflected in the number of tokens within the basic component. For instance, a numerical value such as "2"' in P_{GA_up} means that two basic components are active and operational. Figures 3(c) and 3(d) illustrate the SPN models for the master control stations and monitor stations. The failure and recovery behavior is similar to the one presented for the ground antenna.

5.3 Reliability models

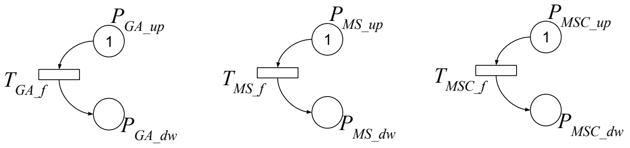
Figure 4 displays the default reliability models for a GNSS. The SPNs, encompassing interconnected sub-networks corresponding to a satellite, a GA, a MS, and a MSC, are similar to the availability models but without considering the repair events. In this model, we introduce P_{N_SSO} to represent spare satellites in the repair orbit, and guard functions are assigned to transitions t_{SSO} and t_{SSO2} to enable the replacement of operational satellites by spare satellites only if there are satellites available in the repair orbit (see Table 1). Additionally, since any component failure renders the GNSS unavailable, we have incorporated guard functions, as described in Table 1, to reflect this aspect.

As the satellite is the most critical and costly component in a satellite constellation, Figures 5 and 6 illustrate the reliability model for this component, while Table 2 illustrates the guard function used in these models. It is worth mentioning that a satellite failure can have significant consequences, affecting the overall functionality and mission success of the satellite constellation. Therefore, understanding and precisely evaluating the reliability of the satellite component is crucial to ensure the robustness and effectiveness of the entire satellite system.

In the first figure, we consider the presence of spare satellites in the repair orbit, representing a cold standby redundancy. The transition T_{S_TMOO} represents the time taken for the satellite to move from the repair orbit to the operational orbit. This time can vary significantly depending on crucial factors such as the propulsion system's capabilities, orbital mechanics involved in the transfer, mission planning strategies,



(a) Satellite Model



(b) Ground Antenna Model (c) Monitor Station Model (d) Master Control Station Model

Fig. 4 Constellation reliability model.

Table 1 Guard functions for the models of Figure 4.

Transition	**Guard expression**
t_{SSO}	$(P_{N\_SSO} = 0)$
t_{SSO2}	$(P_{N\_SSO} >= 1)$
T_{S_Pf}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{S_r1}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{S_Tf}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{S_r2}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{S_Sf}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{S_TMOO}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_{GA\_dw} = 0) AND (P_{S\_dw} = 0)$
T_{GA_f}	$(P_{MS\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_d w = 0)$
T_{MS_f}	$(P_{GA\_dw} = 0) AND (P_{MCS\_dw} = 0) AND (P_d w = 0)$
T_{MSC_f}	$(P_{GA\_dw} = 0) AND (P_{MS\_dw} = 0) AND (P_d w = 0)$

among others. In the second figure, we consider the presence of spare satellites in the operational orbit, constituting a hot standby redundancy. In this scenario, the timed transition (T_{S_TMOO}) from the previous model is replaced by an immediate transition (t_{S_TMOO}), meaning that no time is required for deploying the spare satellite. It is important to note that having a spare satellite in the operational orbit is more expensive due to the increased operational costs associated with maintaining a ready-to-use spare satellite.

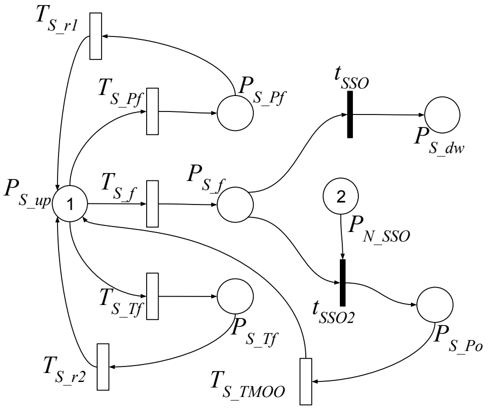


Fig. 5 Reliability model, considering a cold standby redundancy.

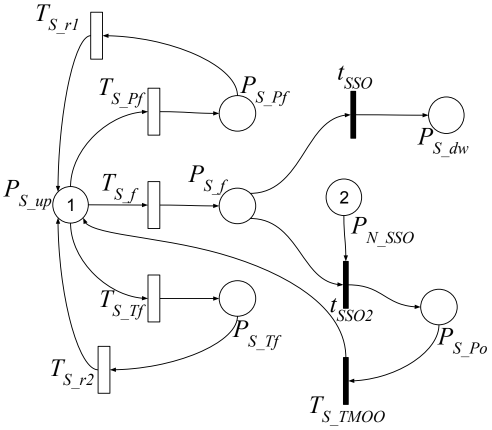


Fig. 6 Reliability model, considering a hot standby redundancy.

Table 2 Guard functions for the models of Figures 5 and 6.

Transition	**Expression**
t_{SSO}	$(P_{N\_SSO} = 0)$
t_{SSO2}	$(P_{N\_SSO} >= 1)$

5.4 Maintainability model

Figure 7 illustrates the default maintainability model for a satellite in a GNSS. Our focus is exclusively on the corrective maintainability of the satellite, since it is the most important and expensive component in a GNSS. When a failure occurs, ground staff assess and determine the most effective repair strategy, which may involve transferring a satellite from a repair orbit to its operational orbit or launching a new satellite from the ground to replace the damaged one. Consequently, this model serves the purpose of calculating various metrics to assess the repair and replacement of satellites. This includes determining the frequency of satellite replacements needed in the operational orbit, considering satellites in repair orbits, as well as the quantity of satellites requiring launch from Earth to sustain the operational constellation. The model is similar to the availability model presented in Figure 3(a), but excludes planned and transient outages represented by the transitions $T_{S_{P}f}$ and $T_{S_{T}f}$. Transient outages refer to temporary interruptions, after which the satellite resumes operational status, while permanent outages require satellite replacement, justifying the removal of these transitions. It is important to note that unlike the availability model, which focuses on the probability of the satellite being operational, our model aims to assess the repair and replacement needs of satellites to sustain the operational constellation.

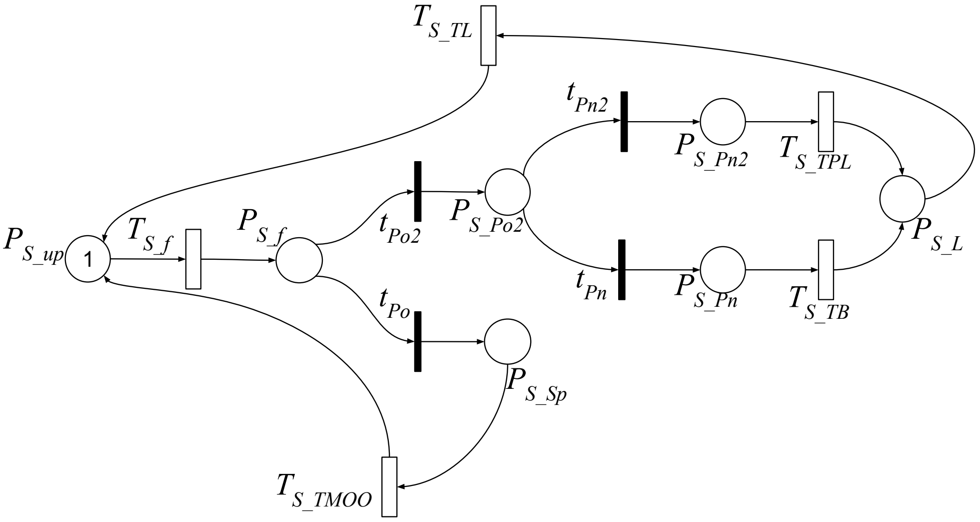


Fig. 7 Maintainability model.

5.5 Adopted metrics

In this study, we consider several key metrics: steady-state availability (AV), reliability of the GNSS (RL_GNSS), reliability of the satellite (RL_S), the number of required satellite replacements in the operational orbit (RO) and the quantity of satellites needing launch from Earth (LE). Table 3 displays the default expressions used to evaluate these metrics, which are defined for the models presented above. It is worth noting that AV is computed through a stationary analysis, where the operational mode requires at least four satellites, one monitor station, one master control station, and one ground antenna for the GNSS to be considered operational. RL_GNSS and RL_S, on the other hand, are determined using transient analysis over a specific period, where the one minus the probability of any component of the GNSS failure is computed.

Finally, RO and LE are calculated by the throughput multiplied by the analysis period represented by P, where S_TMOO and S_TL denote the values assigned to transitions T_{S_TMOO} and T_{S_TL}, respectively. Note that the metrics are computed based on the probabilities of finding a given number of tokens (or the expected number of tokens) in specific places of the SPN models, where $P\{exp\}$ calculates the probability of the inner expression (exp); $\#p$ denotes the number of tokens in place p, and $E\{\#p\}$ computes the expected number of tokens in place p.

Table 3 Expression for evaluating the adopted metrics.

Metric	Expression
AV	$P\{(\#P_{S\_up} >= 4)AND(\#P_{MCS\_up} >= 1)AND(\#P_{GA\_up} >= 1)$ $AND(\#P_{MS\_up} >= 1)\}$
RL_GNSS	$1 - P\{(\#P_{MS\_dw} = 1)OR(\#P_{MCS\_dw} = 1)OR(\#P_{GA\_dw} = 1)OR(\#P_{S\_dw} = 1)\}$
RL_S	$1 - P\{(\#P_{S\_dw} = 1)\}$
RO	$((E\{\#P_{S\_Sp}\}) * (1/S\_TMOO)) * P$
LE	$((E\{\#P_{S\_L}\}) * (1/S\_TL)) * P$

6 Numerical study

In this section, we describe the numerical results obtained from CDA and the models presented in Section 5. Firstly, we discuss the results regarding reliability, followed by availability, and finally, maintainability. Table 4 lists the parameters adopted in the evaluations. These parameters are derived from real values obtained from [11, 18]. Mercury tool [26] was used for modeling and analysis. As will be shown, we do not set any target values for any metrics. Instead, we present an in-depth case study in which different scenarios are considered. Note that the default models from Section 5, along with the default parameters listed in Table 4, are employed for the analysis. Any modifications made to these models or parameters are explicitly stated in the analysis.

6.1 Reliability analysis

The reliability of a GNSS system, defined as the probability of its uninterrupted operation for a period, is crucial for ensuring a dependable service. Figure 8 illustrates how the system's reliability changes over a year, considering different configurations: the default configuration (DFC), redundancy only in the monitor station (RDC in MS), redundancy in both the monitor station and master control station (RDC in MS + MCS), and redundancy in the monitor station, master control station, and ground antenna (RDC in MS + MCS + GA). This analysis adopts the models presented in Figure 4. As shown, system reliability steadily increases with the level of redundancy implemented. The system in its default configuration (DFC) exhibits the lowest reliability. Note that the reliability of the system with DFC and the system with redundancy only in the monitor station (RDC in MS) overlaps significantly. This observation suggests that adding redundancy solely in the monitor station provides minimal improvement. On the other hand, the system with redundancy in the monitor station, master control station, and ground antenna (RDC in MS + MCS +

Table 4 Default input parameters for the dependability models.

Transition	**Value**
T_{S_Pf}	4320 (hrs)
T_{S_Tf}	4320 (hrs)
T_{S_r1}	24 (hrs)
T_{S_r2}	24 (hrs)
T_{S_f}	43830 (hrs)
T_{S_TMOO}	12 (hrs)
T_{S_TB}	4320 (hrs)
T_{S_TPL}	1440 (hrs)
T_{S_TL}	24 (hrs)
T_{GA_f}	2310 (hrs)
T_{GA_r}	4.2 (hrs)
T_{MS_f}	156000 (hrs)
T_{MS_r}	0.42 (hrs)
T_{MSC_f}	1248 (hrs)
T_{MSC_r}	0.8716667 (hrs)
Po	0.9 (prob.)
$Po2$	0.1 (prob.)
Pn	0.9 (prob.)
$Pn2$	0.1 (prob.)

GA) demonstrates the highest reliability. This result shows the significant impact of enhancing redundancy beyond the initial stages of the system's infrastructure.

The findings demonstrate that prioritizing investments in ground-based equipment, such as monitor stations and master control stations, can provide substantial improvements in GNSS system reliability. This is particularly relevant when compared to investments in satellites, which may offer less cost-effective solutions for achieving the desired level of reliability. The observed overlap between the DFC and RDC in MS configurations highlights the importance of carefully analyzing the impact of individual components on overall system reliability. Additionally, the use of CDA facilitates easy adjustments to the number of components, enabling crucial analyses for designers and operators. It is worth noting that the default metric (RL_GNSS) presented in Table 3 need adjustment to consider each redundancy case, as failures occur when no component, including the redundant one, is available. Therefore, Table 5 presents the metrics for RDC in MS, RDC in MS + MCS and RDC in MS + MCS + GA.

Table 5 Expression for evaluating the reliability.

Metric	**Expression**
RDN in MS	$1 - P\{(\#P_{MS\_dw} = 2) OR (\#P_{MCS\_dw} = 1) OR (\#P_{GA\_dw} = 1)$ $OR (\#P_{S\_dw} = 1)\}$
RDN in MS + MCS	$1 - P\{(\#P_{MS\_dw} = 2) OR (\#P_{MCS\_dw} = 2) OR (\#P_{GA\_dw} = 1)$ $OR (\#P_{S\_dw} = 1)\}$
RDN in MS + MCS + GA	$1 - P\{(\#P_{MS\_dw} = 2) OR (\#P_{MCS\_dw} = 2) OR (\#P_{GA\_dw} = 2)$ $OR (\#P_{S\_dw} = 1)\}$

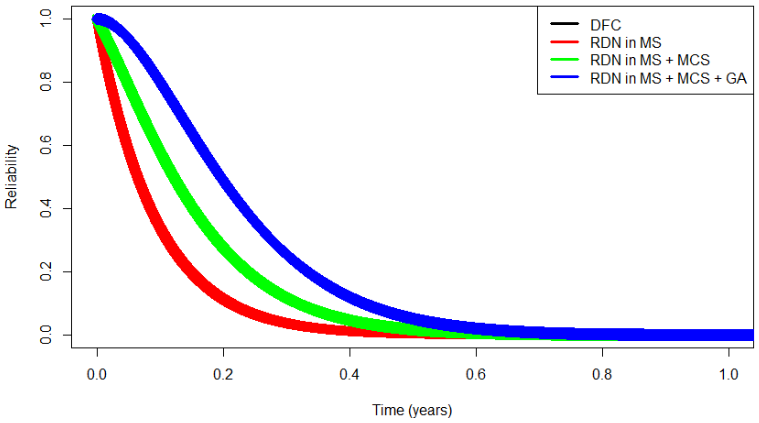


Fig. 8 Reliability analysis of the GNSS.

Considering the satellite as the most critical and costly component in a GNSS, Figures 9 and 10 demonstrate the satellite's reliability over a 10-year period, taking into account the number of redundant satellites in both the repair and operational orbits (cold and hot standby redundancies). This analysis adopts the models presented in Figures 5 and 6, respectively. The results show that the system's reliability decreases rapidly without satellite redundancy, but it remains close to 100% with three or more redundant satellites, regardless of their location in the repair or operational orbit. This finding has significant implications for GNSS designers and operators. It highlights the importance of incorporating redundancy into the system architecture to mitigate the impact of satellite failures. It also suggest that investments in spare satellites can be justified by the resulting improvements in system reliability. Additionally, the location of redundant satellites, whether in the repair or operational orbit, does not significantly impact the overall system reliability. This implies that investments in a hot standby redundancy may not be significant for this scenario, offering considerable cost savings.

6.2 Availability analysis

When a satellite fails, the probability of resolving the failure in orbit by replacing it with a redundant satellite represents the previously obtained reliability for the satellite. Thus, in Figure 11, we illustrate the impact of the reliability on availability. The x-axis represents the varying reliability, ranging from 0.5 up to 1. The results clearly demonstrate a positive correlation between the two variables, meaning that higher satellite reliability translates to higher system availability. For instance, a system with a satellite reliability of 0.5 (50%) exhibits an approximate availability of 0.94, implying that it is expected to be operational approximately 94% of the time. On the other hand, a system with a satellite reliability of 0.9 (90%) achieves an approximate availability of 0.97, meaning it is expected to be operational approximately 97% of the

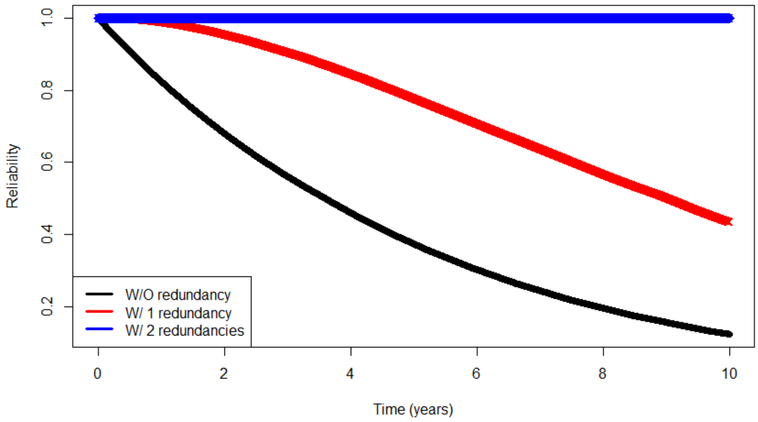


Fig. 9 Reliability analysis of the satellite considering a repair orbit.

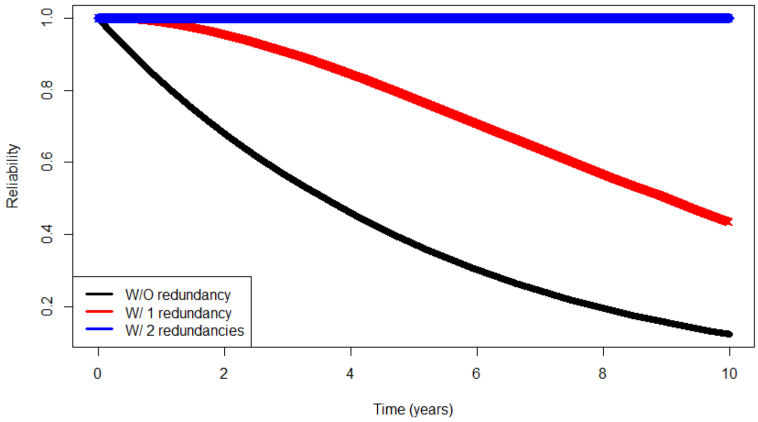


Fig. 10 Reliability analysis of the satellite considering an operational orbit.

time. Understanding and managing this critical relationship between satellite reliability and system availability is essential for GNSS designers and operators to ensure their systems meet the diverse needs of users as well as mission requirements.

A GNSS relies on satellites, each having distinct mean time to failure rates. Thus, in Figure 12, we illustrate the impact of the mean time to failure of a satellite on availability. That is, we vary the value of the transition $T_{S\text{-}f}$ and analyze its impact on the availability metric (AV). The x-axis represents the mean time to failure of a satellite, spanning from 5 to 20 years. As expected, a positive correlation exists between MTTF and availability, where higher MTTF values translate to significantly

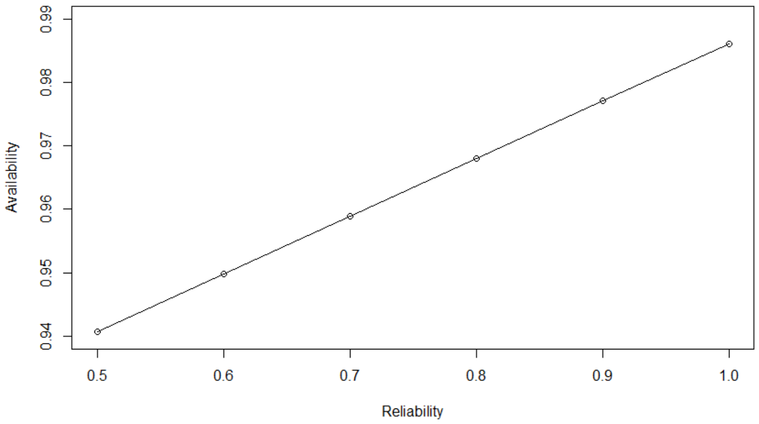


Fig. 11 Impact of the reliability on the availability of the GNSS.

improved system availability. This confirms the necessity of choosing satellites with high MTTF and emphasizes the essential advancements needed in satellite technology and manufacturing processes. These advancements are crucial to achieve longer MTTF values and improve the overall availability of GNSS systems.

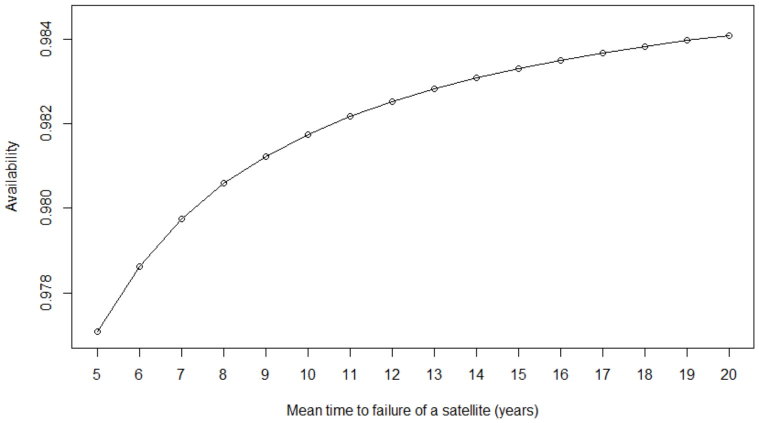


Fig. 12 Impact of the mean time to failure of a satellite on availability.

If a satellite fails, the process involves either utilizing an available redundant satellite in the operational orbit or relocating a redundant satellite from a repair orbit to an operational one. Firstly, let us assume that there are redundant satellites available in the operational orbit. Therefore, in Figure 13, we illustrate the impact of the number of redundant satellites on availability. The x-axis represents the varying number of satellites (P_{S_up}), ranging from 4 to 7. Note that the operational mode specifically considers that, for the satellite, at least four satellites need to be working properly for the GNSS to be considered operational. The results demonstrate a clear positive correlation between the number of spare satellites and system availability. However, the rate of availability stabilizes after exceeding two spare satellites (six satellites), which is consistent with the results presented in Figures 9 and 10. This suggests that a minimal level of redundancy, around two spare satellite, is sufficient to maintain high system availability. This finding has significant implications for GNSS designers and operators. It facilitates them to optimize resource utilization by ensuring the deployment of sufficient spare satellites to achieve high system availability while avoiding unnecessary costs associated with excess spare capacity.

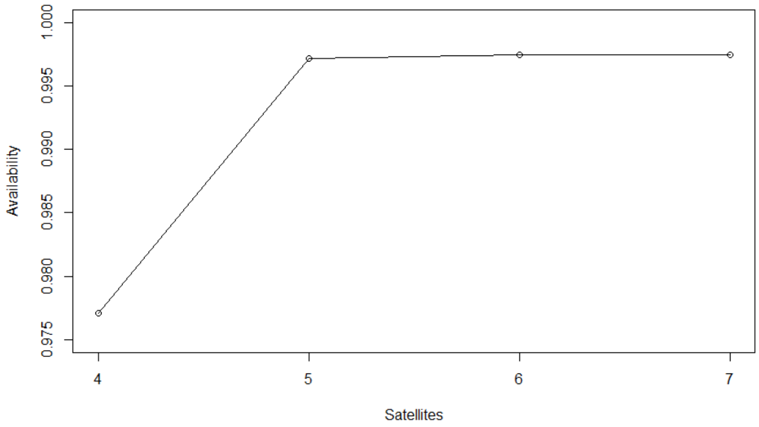


Fig. 13 Impact of the number of redundant satellites on availability.

Secondly, let us consider a scenario where no redundant satellites are available in the operational orbit, requiring the relocation of a redundant satellite from a repair orbit to an operational one. In this analysis, we are interested in evaluating the impact of this relocation, as represented by the transition T_{S_TMOO}. This relocation is influenced by various factors, such as orbital mechanics, propulsion system capabilities, and logistical considerations. Therefore, in Figure 14, we illustrate the impact of the mean time required to transition to the operational orbit on availability. The x-axis represents the varying time for relocation to the operational orbit, ranging from 1 to 24 hours. As expected, shorter relocation times result in higher system availability. This finding is crucial for determining the level of investment needed in factors influencing satellite relocation from the repair orbit to the operational orbit. By optimizing these factors, GNSS designers and operators can achieve faster relocation times, minimizing downtime and ensuring high system availability.

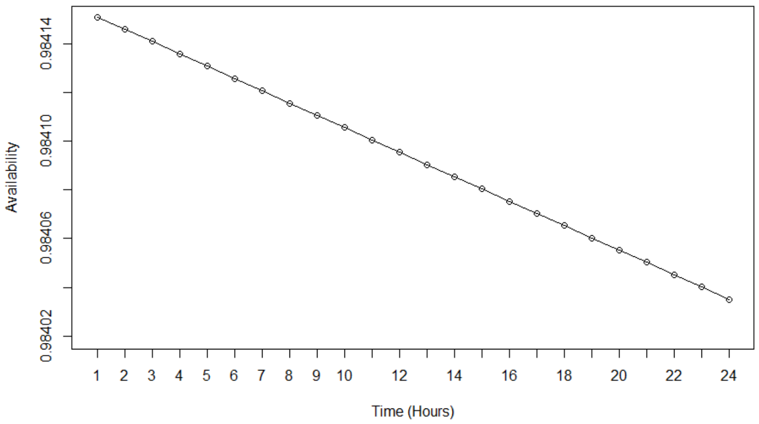


Fig. 14 Impact of the relocation time on availability.

6.3 Maintainability analysis

Maintainability is a critical aspect in satellite operations, and it involves various metrics to assess the repair and replacement requirements. Two key metrics are considered in this context. Firstly, the frequency of satellite replacements required in the operational orbit by satellites in repair orbits (RO). Secondly, the quantity of satellites necessitating launch from Earth to maintain the operational constellation (LE). These metrics, as described in Table 3, are collected from the model presented in Figure 7.

Table 6 illustrates the RO and LE over a 20-year period, considering various probabilities of resolving the failure in orbit (PRF). The table shows that as the PRF increases, RO increases, while LE decreases over the given timeframes of 5, 10, and 20 years. For instance, at a PRF of 0.1 over a 20-year period, the required satellite replacements in the operational orbit amount to 0.056249, significantly lower compared to a PRF of 0.9, where it reaches 3.42. Concurrently, the quantity of satellites needing launch from Earth at a PRF of 0.1 stands at 2.82, reducing to 0 as the PRF reaches 0.006575. These outcomes offer valuable insights for GNSS designers and operators, aiding in more effective mission planning and resource allocation. Understanding how different probabilities of resolving failures affect replacement needs and launch quantities is fundamental for optimizing satellite operations and ensuring sustained system functionality.

6.4 CDA analysis

The analyses conducted by CDA on reliability, availability, and maintainability provided distinct insights into enhancing GNSS system dependability. The examination of the system reliability highlighted the fundamental role of redundancies, particularly in critical system components. It demonstrated that reinforcing redundancies in earth-based infrastructures like monitoring stations, master control systems, and

Table 6 Replacement needs for operational orbit satellites and launch quantity from Earth.

PRF	5 years		10 years		20 years	
	RO	LE	RO	LE	RO	LE
0.1	0.056249	0.705663	0.112497	1.411326	0.224994	2.822652
0.2	0.155962	0.618734	0.311924	1.237467	0.623847	2.474934
0.3	0.256040	0.530526	0.512081	1.061051	1.024161	2.122103
0.4	0.356119	0.440674	0.712238	0.881348	1.424475	1.762697
0.5	0.455832	0.349363	0.911664	0.698723	1.823328	1.397447
0.6	0.555911	0.260241	1.111821	0.520481	2.223642	1.040963
0.7	0.655989	0.175502	1.311978	0.351005	2.623956	0.702011
0.8	0.755702	0.089303	1.511405	0.178607	3.022809	0.357215
0.9	0.855781	0.001644	1.711562	0.003287	3.423123	0.006575

ground antennas resulted in substantial improvements in overall system reliability. This finding highlights the significance of prioritizing investments in ground infrastructures over solely focusing on enhancing satellite redundancies to comprehensively improve system reliability.

A clear correlation between satellite reliability and system availability was evident, emphasizing the necessity of investing in satellite redundancy to ensure high availability. The number of redundant satellites directly affects system availability, showing a saturation point after a specific threshold. Longer MTTF values significantly enhance system availability, necessitating advancements in satellite technology. Maintaining minimal redundancy and expediting satellite transition times are crucial for ensuring consistently high system availability. The maintainability analysis also provided insights into the relationship between the probability of in-orbit failure resolution and the requirements for satellite replacement and launch. Higher probabilities of resolution significantly reduced the number of necessary replacements and satellite launches.

These findings emphasize the importance of utilizing CDA for the design and operation of GNSS. It is crucial not only to consider satellite reliability but also to implement effective redundancies at multiple stages and optimize maintenance strategies to ensure continuous system operation. These insights serve as fundamental guidance for designers and operators in seeking more efficient and reliable solutions for GNSS. For instance, as presented in [27], the performance standard providing the U.S. government's expectations for GPS performance indicates an average availability for the constellation of 0.991. The results obtained in this study closely align with this standard for certain scenarios, as presented in Figure 13, validating the applicability and power of CDA for such analyses and assisting designers and operators in choosing the best GNSS that fits their needs.

7 Conclusion

This study introduced CDA, a strategy based on SPNs for modeling, evaluating, and tuning satellite constellation environments. The proposed models encompass various elements including the launch environment, space and earth components, orbit dynamics, and diverse failure-recovery behaviors. Our approach allows designers and operators to assess trade-offs of different satellite constellation environments, offering more efficient and reliable solutions for GNSS. We conducted a case study, in which we model and evaluate a GNSS. Our findings showed the substantial impact of redundant components on both reliability and availability. Furthermore, they presented how the utilization of satellites in repair and operational orbits can affect these metrics, emphasizing the direct correlation between reliability and maintainability. For future research, we aim to explore the cost trade-offs associated with adopting satellite constellation environments. Additionally, we intend to investigate larger constellations comprising hundreds of elements and develop a user-friendly interface enabling users unfamiliar with Petri nets to model and analyze satellite constellation environments.

References

[1] Kodheli, O., Lagunas, E., Maturo, N., Sharma, S.K., Shankar, B., Montoya, J.F.M., Duncan, J.C.M., Spano, D., Chatzinotas, S., Kisseleff, S., *et al.*: Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials **23**(1), 70–109 (2020)

[2] Bakhtiari, M., Abbasali, E., Daneshjoo, K.: Minimum cost perturbed multi-impulsive maneuver methodology to accomplish an optimal deployment scheduling for a satellite constellation. The Journal of the Astronautical Sciences **70**(3), 18 (2023)

[3] Maral, G., Bousquet, M.: Satellite Communications Systems: Systems, Techniques and Technology. Wiley (2002)

[4] Mariappan, A., Crassidis, J.: Kessler's syndrome: A challenge to humanity. Frontiers in Space Technologies **4** (2023)

[5] Zhai, Y., Joerger, M., Pervan, B.: Continuity and availability in dual-frequency multi-constellation araim. In: Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), pp. 664–674 (2015)

[6] Zhai, Y., Zhan, X., Joerger, M., Pervan, B.: Impact quantification of satellite outages on air navigation continuity. IET Radar, Sonar & Navigation **13**(3), 376–383 (2019)

[7] Avizienis, A., Laprie, J.-C., Randell, B.: Fundamental concepts of dependability. Department of Computing Science Technical Report Series (2001)

[8] Laprie, J.-C.: Dependability: Basic Concepts and Terminology. Springer (1992)

[9] Hapgood, M., Liu, H., Lugaz, N.: SpaceX—Sailing close to the space weather? Wiley Online Library (2022)

[10] Henri, Y.: The OneWeb Satellite System. Springer (2020)

[11] Peng, Z., Lu, Y., Miller, A., Zhao, T., Johnson, C.: Formal specification and quantitative analysis of a constellation of navigation satellites. Quality and Reliability Engineering **32**, 345–361 (2016) https://doi.org/10.1002/qre.1754

[12] Del Portillo, I., Cameron, B.G., Crawley, E.F.: A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. Acta astronautica **159**, 123–135 (2019)

[13] Miller, S., Walker, M.L., Agolli, J., Dankanich, J.: Survey and performance evaluation of small-satellite propulsion technologies. Journal of Spacecraft and Rockets **58**(1), 222–231 (2021)

[14] Lee, Y.-W., Suh, Y.-C., Shibasaki, R.: A simulation system for gnss multipath mitigation using spatial statistical methods. Computers & Geosciences **34**(11), 1597–1609 (2008)

[15] Shi, L., Du, S., Miao, Y., Lan, S.: Modeling and performance analysis of satellite network moving target defense system with petri nets. Remote Sensing **13**(7) (2021) https://doi.org/10.3390/rs13071262

[16] Polli, E.M., Gonzalo, J.L., Colombo, C.: Analytical model for collision probability assessments with large satellite constellations. Advances in Space Research **72**(7), 2515–2534 (2023) https://doi.org/10.1016/j.asr.2022.07.055 . Space Environment Management and Space Sustainability

[17] Kelley, C., Dessouky, M.: Minimizing the cost of availability of coverage from a constellation of satellites: Evaluation of optimization methods. Systems Engineering **7**(2), 113–122 (2004) https://doi.org/10.1002/sys.10059 https://incose.onlinelibrary.wiley.com/doi/pdf/10.1002/sys.10059

[18] Lu, Y., Miller, A., Johnson, C., Peng, Z., Zhao, T.: Availability analysis of satellite positioning systems for aviation using the prism model checker. In: 2014 IEEE 17th International Conference on Computational Science and Engineering, pp. 704–713 (2014). IEEE

[19] Castet, J.-F., Saleh, J.H.: Satellite and satellite subsystems reliability: Statistical data analysis and modeling. Reliability Engineering & System Safety **94**(11), 1718–1728 (2009)

[20] Hiriart, T., Castet, J.-F., Lafleur, J.M., Saleh, J.H.: Comparative reliability of geo, leo, and meo satellites. In: Proceedings of the International Astronautical Congress, IAC-09 D, vol. 1 (2009)

[21] Trivedi, K., Andrade, E., Machida, F.: Combining performance and availability analysis in practice. In: Advances in Computers vol. 84, pp. 1–38. Elsevier, ??? (2012)

[22] Hegarty, C.J., Chatre, E.: Evolution of the global navigation satellitesystem (gnss). Proceedings of the IEEE **96**(12), 1902–1917 (2008)

[23] Hofmann-Wellenhof, B., Lichtenegger, H., Wasle, E.: GNSS–global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More. Springer (2007)

[24] Molloy, M.K.: Performance analysis using stochastic petri nets. IEEE Transactions on computers **31**(09), 913–917 (1982)

[25] Ajmone Marsan, M., Conte, G., Balbo, G.: A class of generalized stochastic petri nets for the performance evaluation of multiprocessor systems. ACM Transactions on Computer Systems (TOCS) **2**(2), 93–122 (1984)

[26] Maciel, P., Matos, R., Silva, B., Figueiredo, J., Oliveira, D., Fé, I., Maciel, R., Dantas, J.: 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 (2017). IEEE

[27] Renfro, B.A., Stein, M., Reed, E.B., Villalba, E.: An analysis of global positioning system standard positioning service performance for 2020. Space and Geophysics Laboratory Applied Research Laboratories The University of Texas at Austin: Austin, TX, USA (2020)