Applying Formal Verification to Assess Galileo Search and Human Rescue Communication Services

Abdelhakim Baouya[1], Brahim Hamid[1], Otmane Ait Mohamed[2], Saddek Bensalem[3]
[1]University of Toulouse, IRIT, France
abdelhakim.baouya@irit.fr, brahim.hamid@irit.fr
[2]Concordia University, CANADA
otmane.aitmohamed@concordia.ca
[3]VERIMAG, Université Grenoble Alpes, Grenoble, France
saddek.bensalem@univ-grenoble-alpes.fr

***Abstract*—The Galileo Search and Rescue system (SAR) is a critical European maritime rescue operation. It uses a network of satellites to determine the location of individuals in distress. Designed to last over 12 years, the system has stable components that adhere to fundamental trustworthiness parameters such as Reliability, Availability, and Maintainability (RAM). These parameters are critical for evaluating rescue performance in situations involving endangered individuals. This paper presents a novel approach that utilizes Continuous-Time Markov Chains (CTMCs) and their formal specification in Continuous Stochastic Logic (CSL) to evaluate the performance of the rescue communication service. Furthermore, the performance of these systems is linked to human reaction time to danger, which we model using a stochastic game. We leverage the PRISM model checker for quantitative analysis, considering degradation scenarios within the communication elements and the evolving status of the distressed person.**

***Index Terms*—Satellite Systems, Reliability, Availability, Maintainability, Games, PRISM**

I. Introduction

Satellite systems have become necessary in modern life, fulfilling an essential role in various sectors, including maritime [1] and military operations [2]. The increasing global demand for reliable communication has driven significant innovation within the space industry [3]. Given the critical nature of these systems, dependability assurance is paramount, including the performance assessment of operational tasks, particularly those related to human rescues, such as search and rescue (SAR) missions [4], [5], [6].

Formal verification [7], [8] is a powerful technique that allows for thorough system analysis to prove the properties that ensure its correct operation. Different formalisms can be used, each suited for specific applications. Typical examples include Markov Decision Processes (MDPs), Continuous-Time Markov Chains (CTMCs), and Concurrent Stochastic Games (CSGs). In contrast to simulation, which relies on analyzing results from many random samples, formal verification provides a mathematically rigorous and exhaustive analysis of the system's behavior.

Our work in this paper illustrates how to effectively model communication efficiency and verify its performance using the PRISM model checker [8]. Although the PRISM probabilistic model checker has been widely applied to verify the correctness and effectiveness of hardware and software designs [9], its application to the specific context of SAR systems has not been addressed. Previous research, including studies [10], [11], [12], [13], has primarily concentrated on assessing the dependability of the satellite itself (e.g., the US GPS Satellite). In contrast, this work focuses on the performance of communication services during request-response interactions between a person in distress and the Galileo satellite system. The Galileo satellite handles requests, communicates with ground services to process them, and dispatches qualified personnel to assist distressed individuals. This work considers different degradation sources as reported in the official documentation [4], [5], [6]. The satellite can be in one of three states: nominal, degraded, or severely degraded. Specific anomalies, such as loss of communication with the ground station, cause each degradation status with elapsed time in such a degradation. These anomalies are collected through availability monitoring as described in [4], [5], [6]. The system model is specified as a Continuous-Time Markov Chain (CTMC) [14]. Assuming constant failure and repair rates for the SAR communication services, the time to failure and repair is modeled as an exponentially distributed random variable. Furthermore, this work introduces a new approach by integrating human factors into the model. Unlike earlier models primarily focused on technological aspects, this research integrates human behavior as a "sensor" within the system [15]. This analysis investigates the crucial role of human factors, such as psychological states and environmental conditions, in the timely transmission of rescue signals. It highlights the significant impact of human behavior, particularly under stress, on the effectiveness of search and rescue (SAR) operations. In addition, we consider a complementary approach that investigates the concept of a Concurrent Stochastic Game

(CSG) [16] to provide a perspective transitioning from a Markov model to a game model. This model examines the interplay between a real-time issue of Galileo Search and Rescue service degradation and humans' physiological and psychological capabilities to respond to danger. By conceding these dynamics, we can enhance the overall efficiency and success of SAR missions.

Outline: The remainder of this paper is structured as follows. Section II reviews related work. Section III provides a brief background on CTMCs and the PRISM language. Section IV presents our proposed modeling approach for SAR systems. We then perform a quantitative analysis of the SAR services scenarios in Section V. Finally, Section VI concludes the paper and suggests directions for future research.

II. Related works

Several works in the literature have addressed the quality and deployment of satellite systems. In [12], the authors propose to use CTMC to model satellite systems, demonstrating how this approach can analyze the impact of different factors, such as solar radiation, on satellite reliability and maintenance. Building upon this work, [10] incorporates Erlang distributions into the CTMC framework to further refine the modeling of maintenance and scrubbing activities. Additionally, [13] broadens the scope by incorporating human capabilities in maintaining satellite systems within a game-theoretical model.

While significant research has focused on the quality and deployment of US GPS satellites, research activities explicitly addressing the reliability and performance of the SAR/Galileo satellite system are less prevalent in the literature. Studies addressing this topic include [17], [18], [19]. In [19], the authors investigate a hybrid communication infrastructure combining terrestrial networks with enhanced Galileo SAR for firefighter missions. Using simulations, they compare the advanced Galileo SAR system with the existing Cospas-Sarsat system. They identify performance metrics and determine the optimal number of Galileo satellites to enhance SAR service quality and minimize emergency response times. The authors in [20] evaluate the performance of four Galileo satellites launched in 2018 during their first year of operational service (to reach 22 satellites). Key performance indicators were analyzed, including signal-in-space status, availability, and ranging accuracy. Results demonstrate high signal health and availability, with minimal signal interruptions. Moreover, the numerical results demonstrate high reliability for the most recent additions to the Galileo satellite constellation. The authors in [18] focus on the development of the SAR/Galileo ground system in Korea, outlining a roadmap strategy for the next-generation search and rescue system with the goal of enhancing rescue efficiency by improving location accuracy and reducing response times. The authors in [17] investigate methods to improve the availability of the Return Link Service (RLS) in the Galileo SAR system. Their proposed solutions utilize Network Coding to improve RLM reception by mitigating signal losses due to harsh weather or obstacles, considering backward compatibility and system complexity. However, none of the reviewed research explicitly addresses the quality of Galileo SAR services from the perspective of reliable intervention, especially regarding the dependability parameters mentioned in the documentation and the psychological status of the person in distress.

III. Preliminaries

Probabilistic Model Checking using PRISM [8] relies on constructing a formal model, typically represented using appropriate storage structures. The verification process is then performed by applying a suite of algorithms implemented within the PRISM engine [21]. For our analysis, we employ Continuous-Time Markov Chains (CTMCs) [14], a well-established modeling technique for evaluating reliability and performance, and Concurrent Stochastic Games (CSGs) [16] to model the stochastic interplay between communication entities.

The PRISM model is composed of a set of modules that can synchronize. Each module is characterized by variables and commands (or transitions). The valuations of these variables represent the state of the module. The behavior of each module is described using a set of commands, each of which follows the following format:

$$[a]\ g\ \rightarrow\ \lambda : u$$

This indicates that if the guard condition g evaluates to true, then the update u is enabled to occur with a rate of λ for action a. A guard is a boolean formula constructed from the module variables. The update u is an evaluation of variables expressed as a conjunction of assignments: $v_i' = val_i + \ldots + v_n' = val_n$ where $v_i \in V$, with V being a set of local and global variables, and val_i are values evaluated via expressions denoted by θ such that $\theta : V \rightarrow \mathbb{D}$, where $\mathbb{D}$ is the domain of the variables.

A. Continuous-Time Markov Chains (CTMCs)

The CTMC involves a set of states and a transition matrix $\mathbf{R} : S \times S \rightarrow \mathbb{R}_{\geq 0}$. The rate specifies the delay before a transition between states s and s' takes place $\mathbf{R}(s, s')$, where the probability between s and s' take within time t is given by the value $1 - e^{-\mathbf{R}(s,s') \times t}$. Based on research using PRISM for CTMC modeling, as outlined in [22], exponentially distributed delays are often considered suitable for modeling electronic component lifetimes and inter-arrival times.

Properties are typically expressed in Continuous Stochastic Logic (CSL) [23], a stochastic variant of the well-known Computational Tree Logic (CTL). For instance, the following property expressed in natural language: *Is the probability of that eventually the system failure occurring within 100 time units is less than 0.001* is expressed as: $P_{<0.001}[F^{\leq 100}\ fail]$ Here, $fail$ is the label that refers to the system failure states. Regarding the reward structure, the property expressed in natural language: *What is the amount of reward accumulated*

over a specific 100 times units ? is expressed in CSL as: $R\{\text{"}up\text{"}\} =?[C \leq 100]$.

B. Concurrent Stochastic Games (CSGs)

CSG [16] is a PRISM model where the formalism is based on the idea that players make choices concurrently in each state and then transition simultaneously. In CSGs, each player controls one or more modules, and the actions that label commands within a player's modules must only be used by that specific player.

The properties related to CSGs are expressed in the temporal logic rPATL [24] (short for reward Probabilistic Alternating Temporal Logic). The property grammar is based on CTL [7], extended with the coalition operator $\langle\langle \mathtt{C} \rangle\rangle$ of ATL [25] and the probabilistic operator P of PCTL [26]. For instance, the following property expressed in natural language: *Players 1 and 2 have a strategy that guarantees the probability of computer shutdown within 100 rounds remains below 0.001, even in the presence of memory failures* is expressed in rPATL as: $\langle\langle 1, 2 \rangle\rangle P_{<0.001}[F\ (fail\ \&\ rounds = 100)]$. Here, `fail` is the label that refers to the system failure states. Regarding the reward structure, the property expressed in natural language: *What is the reward r within 100 rounds to reach* `fail` *for both Players 1 and 2 for a selected strategy?* is expressed in rPATL as: $\langle\langle 1, 2 \rangle\rangle R = ?[F\ (fail\ \&\ rounds = 100)]$.

IV. The SAR/Galileo systems

Figure 1 depicts the SAR/Galileo Services, illustrating the organizational structure of rescue services. The system encompasses multiple components that relay beacon signals from distressed users to rescue authorities. This section presents the system parameters and the formal response mode model.

A. The system model

COSPAS-SARSAT (C/S) is an international satellite-based Search and Rescue (SAR) distress alerting system established in 1979 by the USA, Canada, France, and the former USSR [27]. (See Figure 1). The full documentation is available in [28]. The C/S system comprises:

1) Beacons are 406 MHz radio transmitting devices employed in various applications. These include Emergency Position Indicating Radio Beacons (EPIRBs) and Ship Security Alert Systems (SSAS) for maritime use, Emergency Locator Transmitters (ELTs) and ELT Distress Tracking for aviation, and Personal Locator Beacons (PLBs) for individual use.
2) The space segment includes satellites operating in low Earth orbit, geostationary orbit, and medium Earth orbit, responsible for processing signals transmitted by beacons.
3) A Service Ground Segment (SGS) consists of a geographically distributed set of receiving ground stations known as Local User Terminals (LUTs). This network provides ground segment coverage, allowing the tracking of satellites and the generation of independent location estimates for user beacons.
4) Mission Control Centers (MCC) are crucial in distributing C/S distress alerts globally and configuring the alerts for optimal response.
5) The Sar/Galileo Ground Segment consists of five Reference Beacons (REFBE). These reference beacons distributed across the European coverage Area are used to monitor the performance of the SAR/Galileo Service.

The Galileo Search and Rescue (SAR) Forward link service is capable of receiving signals emitted by C/S compatible 406 MHz distress beacons (Forward Link Alert Message, as FLAM)and relaying this information to a ground segment network, known as the Local User Terminal (LUT), which consists of geographically distributed facilities deployed worldwide. The Return Link Service (RLS) enables the relay of data (Return Link Messages, or RLMs) back to the originating beacon. A primary function of the RLS is to provide the end-user of a distress beacon with automatic acknowledgment, confirming the detection of the alert and the determination of their location by the Search and Rescue (C/S) system.

Upon estimating the beacon's location, the Mission Control Center (MCC) issues an RLM_Request. This request, covering the beacon's confirmed position, is transmitted to a backup MCC (Spanish or French). Subsequently, the RLS generates an RLM Transmission Request (RLMR) based on the original FLAM. The Galileo Core infrastructure processes the RLMR and uplinks the RLM to appropriate Galileo satellites, which are then broadcast to the originating beacon.

Once the beacon receives the RLM, sets a receipt status flag within FLAM. This status flag is then transmitted to the RLSP via the C/S MCC. After the RLSP acknowledges the receipt of the RLM, the Galileo system stops sending further RLMs to the beacon. However, if no acknowledgment of RLM reception is received within 24 hours of the initial RLM request, the Galileo system will continue to transmit RLMs to the beacon.

B. Operational capabilities characteristics

According to [4] and [5], Galileo satellites demonstrate a reliability exceeding 88% over a 12-year lifespan, with an availability of 99.5%. The work in [6] reports that the availability of healthy signals from Galileo is 99.22%, with a recovery time of less than 15 hours. This emphasizes the importance of ensuring timely service recovery. Detection performance, a crucial aspect of the system, refers to the probability of successfully detecting 406 MHz beacon transmissions within the SAR/Galileo coverage area and receiving a valid beacon message at the SAR/Galileo LUT Facilities.

Three service states are defined for the SAR Forward link service in the ECA (European Coverage Area): Nominal, Degraded, and Severely Degraded. Nominal indicates

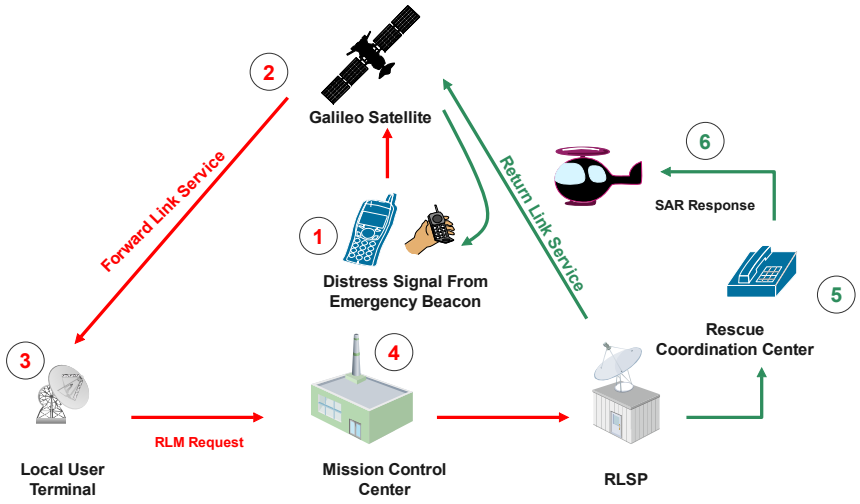

Figure 1: SAR/Galileo Services [4], [5].

normal operation. Degraded is characterized by either non-operational status for less than 24 hours continuously or less than 48 hours cumulatively over a calendar month or by losing communication with one or two ground segments (LUTs) for more than one day, or only 1 REFBE is in nominal status, or no REFBE is operational for less than five continuous days. Severely Degraded occurs when the SGS is non-operational for more than 24 hours continuously or more than 48 hours cumulatively over a calendar month or when communication is lost with all three LUTs and MCCs for more than four hours.

Similarly, the RLS has three service states: Nominal, Degraded, and Severely Degraded. The system is considered "Degraded" if the RLSP is in degraded status or not operational for up to 7 cumulative hours within a calendar month or if RLM messages are delivered but not compliant with the latency MPL: The RLM Delivery Latency within 15 min was above or equal to 99.95% [4]) which means that the Failure Rate is 0.05%, and thus MTTF is 2000 hours. "Severely Degraded" status applies when the RLSP is not operational for more than seven cumulative hours within a calendar month or if RLM messages are not delivered for more than 7 hours. In addition, based on the given availability of 99.8% and the assumption of a very high MTBF, the estimated MTTR for the RLS would be approximately 500 hours.

C. Formal modeling

The SAR/Galileo system can be modeled as a three-state Markov chain, illustrated in Figure 2 and portrayed in the PRISM textual representation in Listing IV.1. State S_1 represents the fully operational system, while state S_2 indicates a faulty state requiring recovery. State S_3 signifies a severe degradation state where maintenance is required. In the PRISM model, the system states are represented by an integer variable S, which can take values from 0 to 3 (line 13). The assignment of degradation status relies on the constant values defined in lines 2-5. In this model, λ

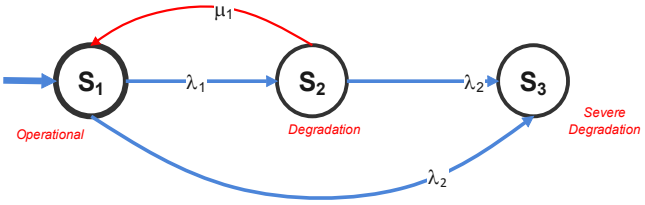

Figure 2: Markov Model Pattern for degradation services in SAR/Galileo Services.

represents the failure rate of system components, and μ_1 indicates the recovery with repair rate. We assume that the rates of constant degradation and severe degradation rates (failure) follow a Poisson process. In Listing IV.1, the parameters are parametrizable as defined in lines 8-10. The reference documentation includes various sources of failure, allowing the model to be parametrized so that users can select which failures impact the communication system. Additionally, this paper discusses how human reliability in sending rescue signals is influenced by their psychological status, which we also model using a Poisson distribution.

V. Quantitative analysis using PRISM

In this work, we focus on evaluating signal transmission performance using the PRISM tool, explicitly focusing on scenarios where the individual experiencing distress maintains a stable psychological status.

a) Experimental setup.: We have encoded properties in CSL formalism and utilized the PRISM model checker v4.8 [29] for verification. These experiments were conducted on an Ubuntu system with an i7 processor and 32GB of RAM. Multiple engines can be selected (refer to documentation [21]), offering performance benefits to specific model structures. In addition, we have implemented the scenarios outlined in [30] to accurately model attack frequencies.

Listing IV.1: The System Status Over Execution Time

```
ctmc
//System states
const int Operational = 2;
const int Degraded = 1;
const int Severely_Degraded = 0;

//System performance rates
const double λ1;
const double λ2;
const double μ1;
//PRISM module
module Degradation
 S : [0..2] init Operational;
 [degradation]       S>0       → λ1:(S'=Degraded);
 [sever_degradation] S>0       → λ2:(S'=
      Severely_Degraded);
 [reset]             S=Degraded→ μ1:(S'=Operational);
endmodule
```

b) Artifacts.: The source code for the experiments described in this section is publicly available on a GitHub repository [31]. The PRISM model comprises eight modules and 28 parameters with 159 lines of code. The website provides detailed instructions for replicating the experiments.

Property 1

$$P =?[G(\text{“up”} \rightarrow F\ !(\text{“up”}))] \qquad \textit{(“Liveness”)}$$

The property *“Liveness”* evaluates the signal performance by calculating the probability of the satellite successfully collecting the signal from a beacon while facing degradation of the signal, represented by the label $!\text{“}up\text{”}$. The results indicate a 100% probability of the system transitioning from a functioning state to a degraded state. Thus, this leads us to investigate the role of degradation features on the signal transmitted through the verification of properties *“Degraded”* and *“Severely Degraded”*.

Property 2

$$P =?[(\text{“up”})\ U^{\leq T}\ (\text{“Degraded”})] \qquad \textit{(“Degraded”)}$$

The property *“Degraded”* specifies that as time elapses, the degradation state increases between the nominal functioning state and the degradation state. However, the primary distinction lies in the specific feature causing the degradation. Figure 3 illustrates that after 10 hours of signal transmission, the probability of degradation reaches 50% and persists at that level for 30 calendar days due to REFBE unavailability. In contrast, internal degradation within 24 hours exhibits a low probability of 3.1%. Notably, combining internal degradation and communication loss with ECA results in a degradation probability of 5.4%. When only one REFBE is operational, the degradation probability reaches 11.6% after 20 hours of execution.

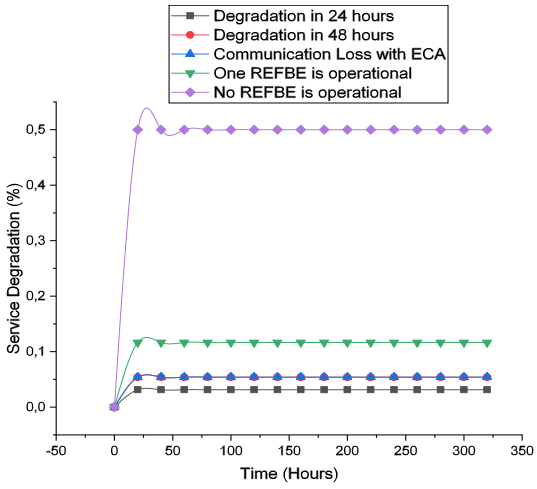

Figure 3: Verification of Property *“Degraded”*.

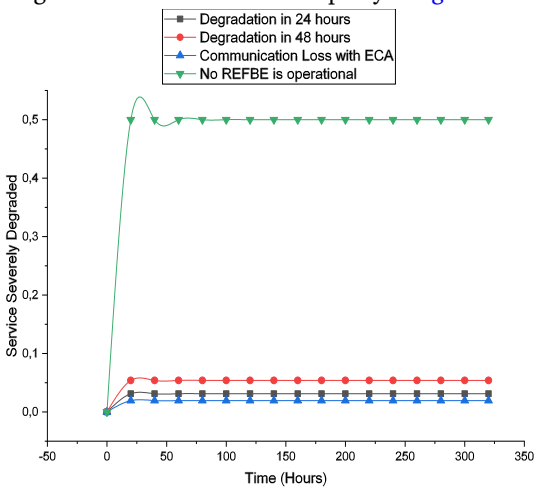

Figure 4: Verification of Property *“Severely Degraded”*.

Property 3

$$P =?[(\text{“up”})\ U^{\leq T}\ (\text{“Severely\_Degraded”})] \qquad \textit{(“Severely Degraded”)}$$

The property *“Severely Degraded”* describes that as the time elapsed between the nominal functioning state and the severe degradation state increases. However, the primary distinction lies in the specific feature causing the degradation, similar to the *“Severely Degraded”* property. Figure 4 illustrates that after 10 hours of signal transmission, the probability of degradation reaches 50% and persists at that level for 30 calendar days due to REFBE unavailability. In contrast, internal degradation within 24 hours and 48 hours exhibits a low probability of 3.1% and 5.4%, respectively. When communication loss with ECA, the severe degradation probability reaches 1.9% less than the degraded mode after 20 hours of execution.

Our analysis has pinpointed the source of service degradation within the SAR/Galileo system. Specifically, issues related to REFBE (Reference Beacon) monitoring of satellite

performance can significantly contribute to service degradation. These problems can also give maintainers erroneous fault results, impacting maintenance activities and quality assurance.

A. Human-in-the-loop

In this study, we examined the performance of the SAR/Galileo system, specifically focusing on degradation issues affecting communication between satellites and the ground stations that assist individuals in distress. The use case is based on existing documentation, and we aim to evaluate the system's capability to save lives by assessing the communication availability of each entity involved in transmitting signals. Although the signal includes multiple parameters not explicitly covered in this study, our emphasis remains on a high-level perspective.

The model can be extended to incorporate other factors influencing satellite signal quality, such as the impact of solar radiation, as discussed in [10], which can significantly affect system reliability. Furthermore, human factors should also be considered, such as an individual's ability to push the distress button in an emergency promptly.

These results do not demonstrate the possibility that the system does not fully encompass the state of the human in terms of their reaction to danger, such as the Mean Time To React to danger (MTTR). To address this limitation, we augment the model with a module that represents the human's status in response to a crisis in a one-month calendar. This module incorporates a formula for the rate of urgent response in line 2 of Listing V.1:

$$\lambda_h = MTTR/Month$$

Consequently, the model is augmented to incorporate human behavior, as illustrated in Listing V.1. Notably, the label "up" encompasses potential human ability degradation. The PRISM command depicts a state transition from the operational mode to a degraded status for the human, upon the value of the degradation rate parameter λ_h in line 6 of Listing V.1. However, the correct status of the communication service depends on the system's status, which can include nominal operation, degradation, severe degradation, and degradation of human factors in line 9.

Listing V.1: The Human Status

```
1  const double time_to_react;
2  const double lambda_h=time_to_react/(30*24);
3
4  module Human_Status
5   Human_Status_s : [0..3] init Operational;
6   [] Human_Status_s>0 -> λh:(Human_Status_s'=Degraded)
        ;
7  endmodule
8
9  label "up" = !degraded & !Severely_Degraded & !(
       Human_Status_s=Degraded);
```

Property 4

$$P =?[(\text{“up”})\ U^{\leq T}\ !(\text{“up”})] \qquad (\text{“Rescue Service”})$$

By examining Property "Rescue Service", which integrates human status, we observe that the system's ability to rescue a person in distress diminishes as the execution time increases, as depicted in Figure 5, regardless of the Mean Time To React (MTTR). This decrease in rescue success is attributed to the increasing likelihood of the individual experiencing a psychological state that hinders their ability to activate the distress button.

While this may seem intuitive, the verification process mathematically confirms this observation. Furthermore, the results demonstrate that the system's effectiveness depends on its capability to rescue the person in danger and crucially relies on the person's timely response to the crisis.

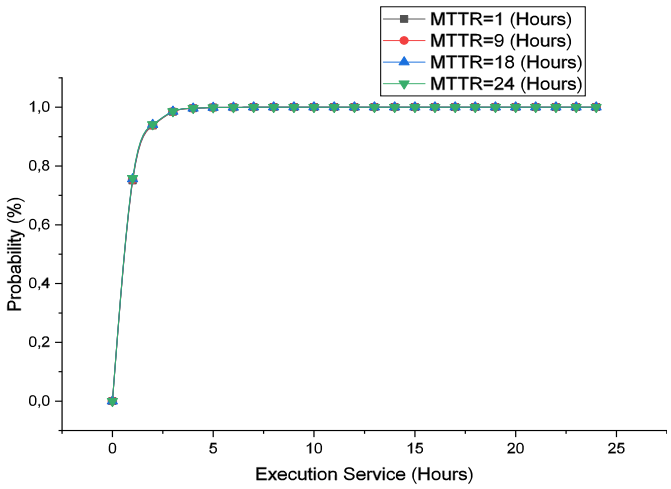

Figure 5: Verification of Property "Rescue Service" with varied MTTR.

B. From a Markov model to a stochastic game model

Previous experiments addressed the issue of human capabilities in responding to rescue services, considering psychological and physiological parameters. In earlier sections, we considered real-time reaction parameters to provide a singular view of the interaction between human and satellite systems. However, Stochastic games verification [16] allows to reason about the interplay as a quantitative correctness assertion about a system's behavior. In our assessment, the discussion centers more on the human capability to react to danger, even when faced with satellite communication failures.

Our model considers the parameters obtained in the previous section as they relate to degradation issues occurring within 24 and 48 hours, communication loss with the ECA, and scenarios in which either one REFBE is operational or none is. The parameters are portrayed in Figure 3 and Figure 4. However, since the degradation of human capabilities is not mentioned in the initial document, it will be considered a parameter.

In Listing V.2, we model human behavior (i.e., the player) using a PRISM module (lines 1-5) that encapsulates both operational and degraded states. The probability of degradation, denoted as *1-ph*, is parametrizable during model checking. However, the likelihood of the satellite system, denoted as *ps*, is collected from previous experiments. In addition, the Observer module, which is a non-player, is in charge of synchronizing the actions between players as it allows for the tracking of degradation. The model is augmented by a module that computes the number of occurrences of players successfully realizing their actions, as represented by the number of rounds. In this game model, the rounds represent the attempted actions performed during the lifecycle to achieve a specific action.

In Listing V.2 lines 21-26, we model a reward structure that captures the uptime and downtime of human and satellite systems. This allows us to calculate communication availability even in the presence of the above failures and human degradation. This measure is expressed in rPATL as follows:

Property 5

$$1 - (\langle\langle 1,2\rangle\rangle \mathrm{R}\{\text{“Uptime”}\}\mathtt{max} =?[\mathtt{F}\ (\mathtt{rounds} = \mathtt{k})] / (\langle\langle 1,2\rangle\rangle \mathrm{R}\{\text{“Uptime”}\}\mathtt{max} =?[\mathtt{F}\ (\mathtt{rounds} = \mathtt{k})] + \langle\langle 1,2\rangle\rangle \mathrm{R}\{\text{“Downtime”}\}\mathtt{max} =?[\mathtt{F}\ (\mathtt{rounds} = \mathtt{k})]))$$

(“Service Availability”)

Listing V.2: CSG Model for Human Interaction with Satellite.

```
1  module Human
2   s1 : [0..2] init Operational;
3   [OPH] s1=Operational -> ph:(s1'=Operational)+(1-ph):(
        s1'=Degraded);
4   [RESET1] s1=Degraded -> (s1'=Operational);
5  endmodule
6
7  module Observer
8  degradation : [0..3] init 0;
9   [RESET1,RESET2] s2=Degraded & s1=Degraded -> (
        degradation'=3);
10  [RESET1,OPS] s1=Degraded & s2=Operational -> (
        degradation'=1);
11  [OPH,OPS] s1=Operational & s2=Operational -> (
        degradation'=0);
12  [OPH,RESET2] s1=Operational & s2=Degraded -> (
        degradation'=2);
13 endmodule
14
15 module SatteliteDegradation
16  s2 : [0..2] init Operational;
17  [OPS] s2=Operational -> ps:(s2'=Degraded)+(1-ps):(s2
        '=Operational);
18  [RESET2] s2=Degraded ->(s2'=Operational);
19 endmodule
20
21 rewards "Uptime"
22         s1=Operational & s2=Operational : 1;
23 endrewards
24 rewards "Downtime"
25         s1=Degraded | s2=Degraded : 1;
26 endrewards
```

We performed verification against the CSG model described in Listing V.2 for Property “Service Availability”, and the results are portrayed in Figure 6. The model checking was performed for different rounds $k := 1..1000$, and the consistent results indicate that the rate remains constant. However, as the degradation of human capabilities regarding their response to danger increases, the efficacy of the communication between the satellite system and the person in danger decreases. This means the severity of the situation increases as the human's capability diminishes. Despite the human's incapacities reaching, for example, 90%, the rescue system is still able to reach the person with a probability close to 40%.

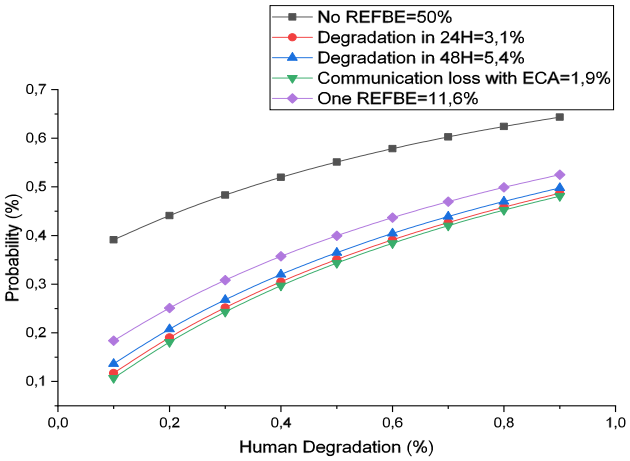

Figure 6: Verification of Property “Service Availability”.

C. Discussion

When comparing our results to those presented in Figure 5, we observe a delta of up to 25% in the worst-case scenario. This discrepancy arises primarily from the fundamental differences in how degradation is modeled in Continuous-Time Markov Chains (CTMCs) versus Concurrent Stochastic Games (CSGs). In CTMCs, degradation is typically characterized by rates, such as MTTR, whereas CSGs require probabilities. This difference in modeling the phenomena leads to distinct observations. Specifically, CSGs inherently capture the strategic interaction where each satellite and the human actor would optimally strive to offer a service. In contrast, CTMCs provide a singular, monolithic view where modules are not modeled as independent, strategic entities.

D. Threats to validity

This paper focuses on specific operational parameters of the SAR/Galileo system. Although other parameters mentioned in this SAR/Galileo documentation could also be verified, the PRISM model checker has limitations in supporting particular formalisms, particularly when incorporating satellite location and accuracy using complex data representation.

VI. Conclusion

This paper presents an approach based on CTMCs and CSGs to model the communication services of the SAR/-Galileo system. The captured model incorporates multiple degradation scenarios related to the observed and monitored communication between satellite systems and ground stations. We leverage the PRISM model checker for quantitative analysis, considering availability parameters and the evolving status of the distressed person.

The analysis assesses which degradation source contributes most significantly to system failures and reduced reliability. Multiple factors were investigated, including loss of communication with monitoring ground stations and monitored failures attributed to human causes or environmental factors (the documentation does not explicitly mention the accurate sources of failures). The results demonstrate that ground stations responsible for monitoring signals are the most active sources of failures. Also, an evaluation has been performed to assess the human's capability to react to the crisis in conjunction with the system status. The results demonstrate that the system and human parameters significantly influence performance in both models. Future work will also involve a comparative analysis of statistical and probabilistic model checkers to investigate the resulting model sizes and the feasibility of verification.

References

[1] Juan A. Fraire, Santiago Henn, Gregory Stock, Robin Ohs, Holger Hermanns, Felix Walter, Lynn Van Broock, Gabriel Ruffini, Federico Machado, Pablo Serratti, and Jose Relloso. Quantitative analysis of segmented satellite network architectures: A maritime surveillance case study. *Computer Networks*, 255:110874, 2024.

[2] Pat Norris. Developments in high resolution imaging satellites for the military. *Space Policy*, 27(1):44–47, 2011.

[3] The Economist. A new constellation of space tie-ups. https://impact.economist.com/projects/a-new-constellation-of-space-tie-ups/, 2024.

[4] European Space Agency (ESA). Galileo performances. https://gssc.esa.int/navipedia/index.php/Galileo_Performances, Accessed in January 2025.

[5] European Union Agency for the Space Programme (EUSPA). Galileo open service system definition document (sdd) v1.3. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OS-SDD_v1.3.pdf, Accessed in January 2025.

[6] European Union Agency for the Space Programme (EUSPA). Galileo open service (os) performance reports. https://www.gsc-europa.eu/electronic-library/performance-reports/galileo-open-service-os, Accessed in January 2025.

[7] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. The MIT Press. OCLC: ocn171152628.

[8] Marta Kwiatkowska, Gethin Norman, and David Parker. PRISM 4.0: Verification of probabilistic real-time systems. In *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)*, volume 6806 of *LNCS*, pages 585–591. Springer, 2011.

[9] PRISM - Bibliography - PRISM model checker. https://www.prismmodelchecker.org/bib.php. [Accessed: July 10, 2024].

[10] Khaza Anuarul Hoque, Otmane Ait Mohamed, and Yvon Savaria. Towards an accurate reliability, availability and maintainability analysis approach for satellite systems based on probabilistic model checking. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1635–1640, 2015.

[11] Yu Lu, Zhaoguang Peng, Alice Miller, Tingdi Zhao, and Chris W. Johnson. How reliable is satellite navigation for aviation? checking availability properties with probabilistic verification. *Reliab. Eng. Syst. Saf.*, 144:95–116, 2015.

[12] Zhaoguang Peng, Yu Lu, Alice Miller, Chris W. Johnson, and Tingdi Zhao. A probabilistic model checking approach to analysing reliability, availability, and maintainability of a single satellite system. In *Seventh UKSim/AMSS European Modelling Symposium, EMS 2013, 20-22 November, 2013, Manchester UK*, pages 611–616. IEEE, 2013.

[13] Abdelhakim Baouya, Brahim Hamid, Otmane Ait Mohamed, and Saddek Bensalem. Model-based reliability, availability, and maintainability analysis for satellite systems with collaborative maneuvers via stochastic games. In *2024 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, pages 27–34, 2024.

[14] Marta Kwiatkowska, Gethin Norman, and David Parker. *Stochastic Model Checking*, pages 220–270. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[15] D. Nunes, J.S. Silva, and F. Boavida. *A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems*. IEEE Press. Wiley, 2018.

[16] Marta Kwiatkowska, Gethin Norman, David Parker, and Gabriel Santos. Equilibria-based probabilistic model checking for concurrent stochastic games. In *Formal Methods – The Next 30 Years*, pages 298–315, Cham, 2019. Springer International Publishing.

[17] R. Alegre-Godoy and I. Stojkovic. Improving the availability of the sar/galileo return link service via network coding. In *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–6, 2014.

[18] Inone Joo, Sanguk Lee, and Jae-Hoon Kim. Study on development strategy for sar/galileo ground system in korea. In *2007 International Conference on Control, Automation and Systems*, pages 2546–2549, 2007.

[19] Andreas Lewandowski, Brian Niehoefer, and Christian Wietfeld. Performance evaluation of satellite-based search and rescue services: Galileo vs. cospas-sarsat. In *2008 IEEE 68th Vehicular Technology Conference*, pages 1–5, 2008.

[20] Constantin-Octavian Andrei, Jan Johansson, Hannu Koivula, and Markku Poutanen. Signal performance analysis of the latest quartet of galileo satellites during the first operational year. In *2020 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6, 2020.

[21] PRISM Development Team (eds.). Prism manual. https://www.prismmodelchecker.org/manual/ConfiguringPRISM/ComputationEngines. Accessed: July 10, 2024.

[22] PRISM Model Checker. Prism - publications. https://www.prismmodelchecker.org/casestudies/index.php#reliability. [Accessed: January 10, 2025].

[23] Marta Kwiatkowska, Gethin Norman, and David Parker. Approximate symbolic model checking of continuous-time markov chains. In *Proceedings of the 14th International Conference on Concurrency Theory*, pages 51–65. Springer, 2002.

[24] Taolue Chen, Vojtěch Forejt, Marta Kwiatkowska, David Parker, and Aistis Simaitis. Automatic verification of competitive stochastic systems. In *Tools and Algorithms for the Construction and Analysis of Systems*, volume 7214, pages 315–330. Springer Berlin Heidelberg.

[25] Rajeev Alur, Thomas A. Henzinger, and Orna Kupferman. Alternating-time temporal logic. *J. ACM*, 49(5):672–713, sep 2002.

[26] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. 6(5):512–535.

[27] European GNSS Agency (GSA). Search and rescue (sar) - galileo service. https://www.gsc-europa.eu/galileo/services/search-and-rescue-sar-galileo-service, Accessed in February 2025.

[28] European Union Agency for the Space Programme (EUSPA). Galileo search and rescue service definition document (sdd). https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-SAR-SDD.pdf, Accessed in January 2025.

[29] Marta Kwiatkowska, Gethin Norman, David Parker, and Gabriel Santos. Prism-games 3.0: Stochastic game verification with concurrency, equilibria and time. In *Computer Aided Verification*, pages 475–487, Cham, 2020. Springer International Publishing.

[30] Quanyan Zhu and Tamer Başar. Dynamic policy-based ids configuration. In *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, pages 8600–8605, 2009.

[31] Abdelhakim Baouya. Paper Artefacts Sources. https://hermes-design.github.io/seaa2025.html.