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

Abdelhakim Baouya[1], Brahim Hamid[1], Otmane Ait Mohamed[2], and Saddek Bensalem[3]

[1] IRIT, Université de Toulouse, CNRS, UT2, France
abdelhakim.baouya@irit.fr, brahim.hamid@irit.fr
[2] HVG Group, ECE Department, Concordia University, Montréal, Canada
otmane.aitmohamed@concordia.ca
[3] VERIMAG, Université Grenoble Alpes, CNRS, Grenoble, France
saddek.bensalem@univ-grenoble-alpes.fr

Abstract. The Galileo Search and Rescue (SAR) system is a cornerstone of European maritime rescue operations. It leverages a network of satellites to pinpoint the location of individuals in distress. With a designed lifespan exceeding 12 years, the system relies on robust components with inherent dependability parameters such as Reliability, Availability, and Maintainability (RAM). These parameters are crucial for assessing the overall rescue performance in situations involving individuals in danger. This paper presents a novel approach utilizing Continuous-Time Markov Chains (CTMCs) and their formal specification in Continuous Stochastic Logic (CSL). We leverage the PRISM model checker for quantitative analysis, considering degradation scenarios within the communication elements and the evolving status of the distressed person.

Keywords: Galileo Search and Rescue· Reliability· Availability· Maintainability· PRISM

1 Introduction

Satellite systems have become indispensable in modern life, fulfilling a crucial role in diverse sectors, including maritime [15] and military operations [25]. The increasing global demand for reliable communication has driven significant innovation within the space industry [9]. Given the critical nature of these systems, dependability assurance is paramount. This includes the performance assessment of operational tasks, particularly those related to human rescue, such as search and rescue (SAR) missions [11,13,12].

Formal verification [20] is a powerful technique for performance and dependability assessment of critical and complex systems. It focuses on probabilistic model checking, which involves constructing and analyzing probabilistic models, typically Markov chains or Markov processes [4]. Various formalisms can be employed, each suitable for specific use cases. Common 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 ~~obtained~~ from ~~a large number of~~ random samples, formal verification provides a mathematically rigorous and exhaustive analysis of the system's behavior.

~~This~~ paper ~~demonstrates~~ how to ~~accurately~~ model communication efficiency and verify its performance using the PRISM model checker [20] . ~~While~~ the PRISM probabilistic model checker has been widely applied to verify the correctness and effectiveness of hardware and software designs [1], its application to the specific context of SAR systems has been limited. Previous research, ~~such as~~ [16,23,27,5], has ~~focused~~ on ~~evaluating~~ the dependability of the satellite itself (e.g., the US GPS Satellite). ~~This~~ work focuses on the performance of communication services ~~in the context of~~ request-response interactions between a person in distress and the Galileo satellite system. The Galileo satellite ~~is responsible for handling the request~~, ~~interacting~~ with ground services to process it, and ~~dispatching~~ qualified personnel to ~~intervene and save the person in distress~~. This work considers ~~multiple sources of degradation~~ as reported in the official documentation [11,13,12]. 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 degradation. These anomalies are collected through availability monitoring as described in [11,13,12]. The system model is specified as a Continuous-Time Markov Chain (CTMC) [19]. Assuming constant failure and repair rates for the SAR communication services, the time to failure and ~~time to~~ repair are modeled as exponentially distributed random variables. ~~In addition~~, this work introduces a ~~novel~~ approach by integrating human factors into the model. Unlike ~~previous~~ models primarily focused on technological aspects, this research ~~incorporates~~ human behavior as a~~n~~ "sensor" within the system [26]. ~~Specifically, it considers how human factors, such as psychological state and environmental conditions, can influence the timely transmission of rescue signals. This approach acknowledges that human behavior, particularly in stressful situations, can significantly impact the overall effectiveness of the SAR system. We model the human response time to emergencies using a Poisson process, acknowledging the impact of psychological factors on human behavior during stressful events.~~

Outline The remainder of this paper is structured as follows. Section 2 reviews related work. Section 3 provides a brief background on CTMCs and the PRISM language. Section 4 presents our proposed modeling approach for SAR systems. We then perform a quantitative analysis of the SAR services scenarios in Section 5. Finally, Section 6 concludes the paper and suggests directions for future research.

2 Related works

Several works in the literature have addressed the ~~quality~~ of satellite systems ~~and their deployment~~. In [27], the authors propose ~~modeling~~ satellite systems

using CTMCs, demonstrating how this approach can be used to analyze the impact of various factors, including solar radiation, on satellite reliability and maintenance. Building upon this work, [16] incorporates Erlang distributions into the CTMC framework to further refine the modeling of maintenance and scrubbing activities. Extending these studies, [28] focuses on modeling the reliability of an entire satellite constellation using CTMCs. Furthermore, [5] expands the scope by incorporating human capability in maintaining satellite systems within a game model.

While extensive research has focused on the quality and deployment of US GPS satellites, research activities specifically addressing the Reliability, Availability, and Maintainability (RAM) of the SAR/Galileo satellite system are less prevalent in the literature. Relevant works include [3,17,22]. In [22], the authors investigate a hybrid communication infrastructure combining terrestrial networks with enhanced Galileo SAR for firefighter missions. Through simulations, they compare the enhanced Galileo SAR system with the existing Cospas-Sarsat system, identifying performance indicators and deriving the optimal number of Galileo satellites to improve SAR service quality and reduce response times in emergency situations. The authors in [17] 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 [3] investigate methods to improve the availability of the Return Link Service (RLS) in the Galileo SAR system. The proposed solutions, which leverage Network Coding, aim to enhance RLM reception by mitigating signal losses due to harsh weather or obstructions, while carefully considering backward compatibility and system complexity. None of the reviewed research explicitly addresses the quality of Galileo SAR services from the perspective of reliable intervention, considering both the dependability parameters outlined in the documentation and the psychological status of the person in distress.

3 Preliminaries

Probabilistic Model Checking using PRISM [20] 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 [10]. For our analysis, we employ Continuous-Time Markov Chains (CTMCs) [19], a well-established modeling technique for evaluating reliability and performance. The CTMC involves a set of states and a transition matrix $\mathbf{R} : S \times S \to \mathbb{R}_{\geq 0}$. 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 [8], exponentially distributed delays are often considered suitable for modeling electronic component lifetimes and inter-arrival times.

The PRISM model is composed of a set of modules that can synchronize. Each module is characterized by ~~a set of~~ variables and commands (or transitions). The valuations of these variables represent the state of the module. A set of commands is used to describe the behavior of each module. A command takes the form:

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

This means that if the guard g is true, then an update u is enabled with a rate λ for an action a. A guard is a boolean formula constructed from the module variables. The update u_i 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.

Two types of reward functions are highlighted. The action reward function assigns a real value to each state-action. This value is accumulated when the action a is selected in the state s. Additionally, the state reward function, denoted as $r_S : S \longrightarrow \mathbb{R}$, assigns a real value to each state s. This value is accumulated when the state s is reached.

Properties are typically expressed in Continuous Stochastic Logic (CSL) [18], 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: $R\{\text{"}up\text{"}\} =?[C \leq 100]$.

4 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.

4.1 The system model

COSPAS-SARSAT (C/S) is an international satellite system for Search and Rescue (SAR) distress alerting established in 1979 by the USA, Canada, France, and the former USSR (See Figure 1). The full documentation is available in [14]. The C/S system comprises:

1. Beacons are 406 MHz radio transmitting devices, including Emergency Position Indicating Radio Beacons (EPIRBs) and Ship Security Alert Systems (SSAS) for maritime applications, Emergency Locator Transmitters (ELTs) and ELT Distress Tracking for aviation applications, and Personal Locator Beacons (PLBs) for personal use.

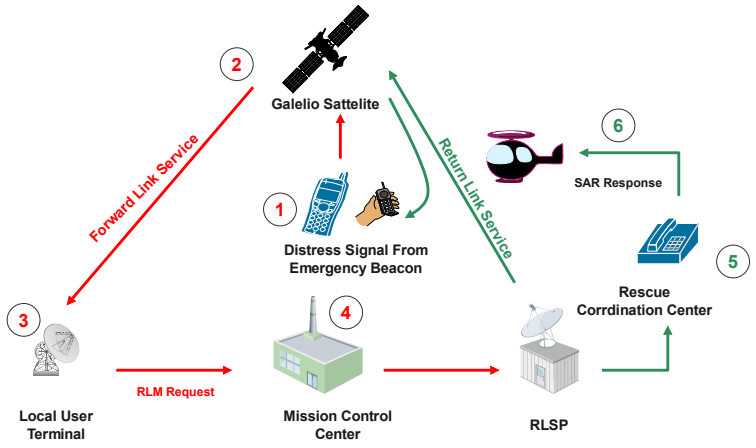

Fig. 1: SAR/Galileo Services [11,13].

2. The space segment ~~comprises~~ 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) ~~comprises~~ a geographically distributed set of receiving ground stations known as Local User Terminals (LUTs). This network provides ground segment coverage, ~~enabling~~ 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 ~~includes~~ five Reference Beacons (REFBE)~~. These reference beacons disseminated over~~ 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 ~~then~~ processes the RLMR and uplinks the RLM to ~~suitable~~ Galileo ~~satellites until it is~~ broadcast to the originating beacon.

~~After receiving an RLM, the beacon~~ sets ~~an RLM~~ receipt status flag within FLAM. This status flag is then transmitted to the RLSP via the C/S MCC. ~~Once~~ the RLSP acknowledges the receipt of the RLM, the Galileo system ~~ceases~~ further ~~RLM transmissions~~ to the beacon. However, if ~~no acknowledgment of~~ RLM ~~reception is received~~ within 24 hours of the initial RLM request, the Galileo system ~~continues~~ to transmit RLMs to the beacon.

4.2 Operational capabilities characteristics

According to [11] and [13], Galileo satellites ~~exhibit~~ a reliability exceeding 88% over a 12-year lifespan ~~and~~ an availability of 99.5%. ~~While~~ [12] ~~indicates a Galileo healthy signal availability of 99.22%~~ with a recovery time of less than 15 hours~~, ensuring timely service recovery remains crucial~~. Detection performance, a ~~key~~ aspect of the system, ~~represents~~ 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 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 5 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% [11]) 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 7 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.

4.3 Formal modeling

The SAR/Galileo system can be modeled as a three-state Markov chain, illustrated in Figure 2. State S_1 represents the fully operational system~~. State~~ S_2

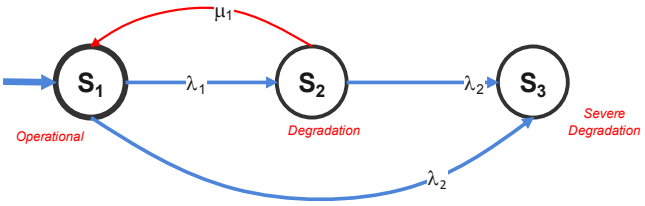

Fig. 2: Markov Model Pattern for SAR/Galileo Services.

~~represents~~ a faulty state requiring recovery. State S_3 ~~represents~~ a severe degradation state where maintenance is required. In this model, λ represents the failure rate of system components, and μ_1 ~~represents~~ the recovery with repair rate. We ~~assume~~ constant degradation and severe degradation rates (failure) follow a Poisson process. The reference documentation includes ~~multiple~~ sources of failure; ~~the~~ model can be parametrized ~~to allow the user to~~ select which failures ~~degrade~~ the communication system. ~~At the discussion level of the paper, we consider human reliability in sending rescue signals to be~~ influenced by their psychological status, which we also model using a Poisson distribution.

5 Quantitative analysis using PRISM

~~The PRISM tool can evaluate a wide range of dependability properties.~~ In this ~~work~~, we ~~are particularly interested~~ in evaluating signal transmission ~~performance~~, ~~specifically~~ focusing on scenarios where the individual experiencing distress maintains a ~~good~~ psychological ~~status~~.

Experimental setup. ~~Within the set of performance properties, we~~ have encoded ~~properties~~ in CSL formalism~~.~~ PRISM model checker v4.8 [21] ~~is utilized to perform~~ verification. ~~These~~ experiments were conducted on a ~~Ubuntu-I7~~ system ~~equipped with~~ 32GB RAM. Multiple engines can be selected (refer to documentation [10])~~ offering~~ performance benefits ~~for~~ specific model structures. In addition, we have implemented the scenarios outlined in [29] to accurately model attack frequencies.

Artifacts. The source code for the experiments described in this section is publicly available on a GitHub repository [2]. The website provides ~~comprehensive~~ instructions ~~on how to replicate~~ the experiments.

Property 1

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

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 !“*up*”. 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*.

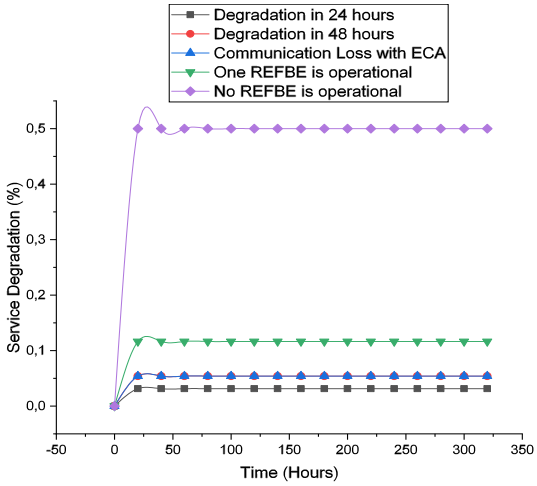

Fig. 3: Verification of Property *Degraded*.

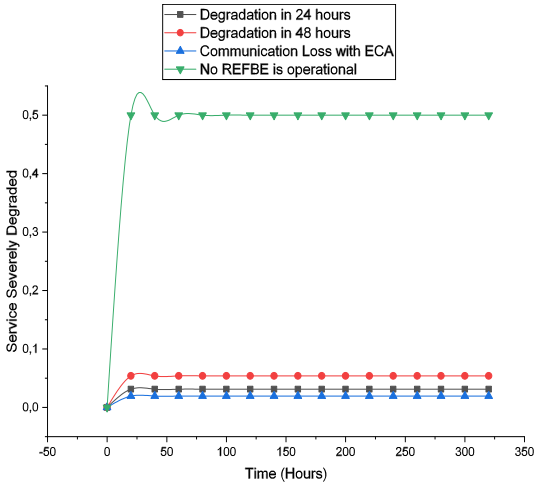

Fig. 4: Verification of Property *Severely Degraded*.

Property 2

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

The property *Degraded* ~~demonstrates~~ that as time elapsed between the nominal functioning state and the degradation state increases. 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.

Property 3

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

The property *Severely Degraded* ~~demonstrates~~ that as 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 ~~and is much similar to the property *Severely Degraded*~~. 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.

Through our analysis, we have ~~identified~~ the source of service degradation within the SAR/Galileo system. ~~Notably~~, issues related to REFBE (Reference Beacon) monitoring of satellite performance can significantly contribute to service degradation. These ~~issues~~ can also provide maintainers with erroneous fault results, impacting maintenance activities and quality assurance.

5.1 Discussion

~~This paper addresses~~ the performance of the SAR/Galileo system, specifically focusing on degradation issues ~~related to~~ communication ~~systems~~ between satellites and the ground stations ~~responsible for assisting~~ ~~persons~~ in distress. The use case is ~~derived from~~ existing documentation, and we ~~intend~~ to ~~address~~ the system's ~~ability~~ to save lives by ~~considering~~ the ~~availability of each entity in communicating its signals~~. ~~While~~ the signal ~~encompasses~~ multiple parameters not explicitly ~~discussed~~ in this study, our ~~focus~~ 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 [16,6], which can significantly affect system reliability. Furthermore, human factors should also

be considered, such as an individual's ~~reliability~~ to ~~promptly~~ push the distress button in an ~~emergency~~.

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:

$$\lambda_h = MTTR/Month$$

So, the model is augmented by human behavior, as shown in Listing 1.1, and the label "Rescued" includes human ability degradation.

Listing 1.1: The Human Status

```
1  module Human_Status
2      Human_Status_s : [0..3] init 3;
3      [] Human_Status_s>0 -> lambda_h:(Human_Status_s'=Degraded);
4  endmodule
5
6  label "up" = !degraded & !Severely_Degraded & !(Human_Status_s=Degraded);
```

Property 4

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

By checking Property Rescue, which integrates the human status in the no-degradation status. we observe that the system's ability to rescue the person in distress decreases as the MTTR increases (within time windows of T=0.5 and T=0.1 of Figure 5). 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.

5.2 Threats to validity

This paper ~~addresses a subset of~~ operational parameters ~~of~~ the SAR/Galileo system. ~~While~~ other parameters ~~referenced~~ in this SAR/Galileo documentation could ~~be considered for verification~~, the PRISM model checker has limitations in supporting particular formalisms, ~~such as~~ incorporating satellite location and accuracy using complex data representation. These parameters necessitate high-level language specifications. ~~Notably, the~~ BIP [7] (Behavior-Interaction-Priority) language can ~~embody~~ these parameters and ~~perform~~ verification using a dedicated statistical model checking with SMC-BIP [24].

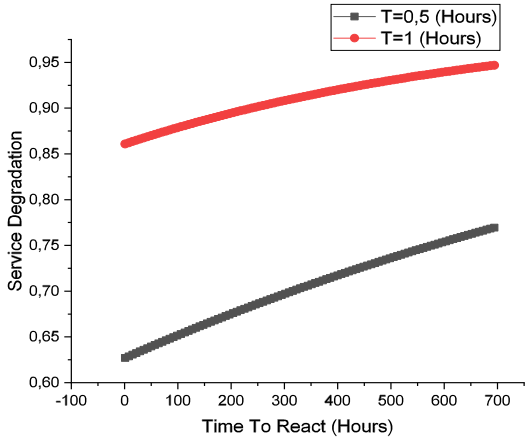

Fig. 5: Verification of Property Rescue wit MTTR.

6 Conclusion

This paper presents an approach based on CTMCs to model the communication services of the SAR/Galileo system. The captured model incorporates multiple degradation scenarios related to the observed and monitored satellite systems' communication with ground stations. We leverage the PRISM model checker for quantitative analysis, considering availability parameters and the evolving status of the distressed person. An evaluation has been performed to assess the human's capability to react to the crisis ~~situation~~ in conjunction with the system status. The results demonstrate that the system ~~performance is significantly influenced by both system~~ and human parameters~~.~~ Future work will consider incorporating additional parameters, such as the number of workstations, and exploring the implications of other formalisms, such as stochastic games, for assessing the reliability of human behavior in distress.

References

1. PRISM - Bibliography - PRISM model checker. https://www.prismmodelchecker.org/bib.php. [Accessed: July 10, 2024].
2. Abdelhakim Baouya. Paper Artefacts Sources. https://hermes-design.github.io/iceccs2025.html.
3. 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.
4. Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. The MIT Press. OCLC: ocn171152628.

5. 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.
6. 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 *The 50th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA)*, 2024.
7. Ananda Basu, Saddek Bensalem, Marius Bozga, Jacques Combaz, Mohamad Jaber, Thanh-Hung Nguyen, and Joseph Sifakis. Rigorous component-based system design using the BIP framework. 28(3):41–48.
8. PRISM Model Checker. Prism - publications. https://www.prismmodelchecker.org/casestudies/index.php#reliability. [Accessed: January 10, 2025].
9. The Economist. A new constellation of space tie-ups. https://impact.economist.com/projects/a-new-constellation-of-space-tie-ups/, 2024.
10. PRISM Development Team (eds.). Prism manual. https://www.prismmodelchecker.org/manual/ConfiguringPRISM/ComputationEngines. Accessed: July 10, 2024.
11. European Space Agency (ESA). Galileo performances. https://gssc.esa.int/navipedia/index.php/Galileo_Performances, Accessed in January 2025.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. Marta Kwiatkowska, Gethin Norman, and David Parker. *Stochastic Model Checking*, pages 220–270. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
20. 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.
21. 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.
22. 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.
23. 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.
24. Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, Mahieddine Dellabani, Axel Legay, and Saddek Bensalem. SBIP 2.0: Statistical model checking stochastic real-time systems. In *Automated Technology for Verification and Analysis*, volume 11138, pages 536–542. Springer International Publishing.
25. Pat Norris. Developments in high resolution imaging satellites for the military. *Space Policy*, 27(1):44–47, 2011.
26. D. Nunes, J.S. Silva, and F. Boavida. *A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems*. IEEE Press. Wiley, 2018.
27. 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 David Al-Dabass, Alessandra Orsoni, and Zheng Xie, editors, *Seventh UKSim/AMSS European Modelling Symposium, EMS 2013, 20-22 November, 2013, Manchester UK*, pages 611–616. IEEE, 2013.
28. Zhaoguang Peng, Yu Lu, Alice Miller, Chris W. Johnson, and Tingdi Zhao. Risk assessment of railway transportation systems using timed fault trees. *Qual. Reliab. Eng. Int.*, 32(1):181–194, 2016.
29. 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.