INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 1, PP. 39-44
Manuscript received November 14, 2023; revised March, 2024. doi: 10.24425/ijet.2024.149512

Dependability model of automated intelligent regenerative life support system for space missions

Igor Kabashkin and Sergey Glukhikh

***Abstract*—Long-duration human space missions require intelligent regenerative life support systems that can recycle resources and automatically manage failures. This paper explores using Petri nets to model the reliability and complex interactions of such closed-loop systems. An architecture consisting of primary systems, backups, and consumable reserves is outlined. The automation system that controls everything is described. Petri nets can capture concurrency, failure modes, redundancy, and dynamic behavior. A modular modeling methodology is presented to develop hierarchical Petri net models that scale in fidelity. Elementary fragments represent failures and redundancy. Subsystem modules can be substituted for more detailed models. Analysis and simulation assess system reliability and failure response. This supports designing ultra-reliable systems to safely sustain human life in space.**

***Keywords*—life support system; dependability; automation; modelling; Petri net**

I. Introduction

AS humans look towards longer duration space travel and establishing permanent habitats in space, developing effective life support systems (LSS) is crucial. Traditional life support systems like those used on the International Space Station are not well suited for these long-term missions. They require frequent resupply missions from Earth to provide consumables like oxygen, water, and food. Intelligent regenerative life support systems offer a solution by recycling these resources and even producing new ones through biological and chemical processes.

A key component of an intelligent regenerative system is the integration of various subsystems that can work together autonomously to maintain a habitable environment. This includes atmosphere management, water purification, waste management, food production, and thermal control subsystems. Each subsystem monitors conditions, anticipates needs, self-regulates, and integrates data with the other systems. For example, the atmosphere management system which provides oxygen could monitor crew oxygen consumption and carbon dioxide production. It could then adjust the rate at which carbon dioxide is removed from the air and oxygen produced to precisely meet crew metabolic needs.

The waste management system works hand-in-hand with the food production system. Inedible biomass from the food system can be fed into the waste processor along with human metabolic waste like carbon dioxide, urine, and feces. Through pyrolysis, this waste gets converted into nutrient rich soils that can support crops in the food production unit. The water purification system reclaims water from waste streams and atmospheric condensate to supply the food system and crew needs.

Sophisticated artificial intelligence (AI) and machine learning algorithms help the entire life support system run efficiently by coordinating all the subsystems. The AI can project resource needs into the future, detect any imbalance early, and self-correct. It can also optimize energy and mass flows. If one subsystem has excess heat or oxygen, the AI could route it to where there is a need. This level of automation and integration is what makes an intelligent regenerative life support system uniquely suited for sustainable extraterrestrial habitation. It dramatically reduces dependence on supplies from Earth which is a key capability required for humanity's long-term expansion into space.

Reliability is critically important for intelligent regenerative life support systems since human lives depend on these systems functioning properly. Failure of life support systems could quickly lead to loss of crew if backups are not adequate. As missions go further from Earth, the ability to abort or get resupplied in case of failures becomes increasingly difficult. Therefore, reliability models and metrics are essential tools to design and evaluate life support systems.

The paper proposes one of the approaches to the analysis of the reliability of the considered class of systems, which is the development of the method proposed in the article [1].

II. Related Works

Reliability analysis is critical for intelligent regenerative life support systems to ensure crew safety and mission success. These closed-loop ecosystems have complex interactions and failure modes that must be thoroughly modeled and understood. Quantifying reliability over the lifetime guides design choices and redundancy requirements. Reliability modeling identifies high risk components and predicts the likelihood of losing critical functions. For manned missions far from Earth, where

Igor Kabashkin and Sergey Glukhikh are with Transport and Telecommunication Institute, Latvia (e-mail: kiv@tsi.lv, interbiotechnology@gmail.com).

aborts or resupply are impossible, the ultra-reliable operation of life support systems becomes paramount.

Today there are several reliability modeling techniques that can be applied to life support systems:

- Probabilistic risk assessment models like fault tree analysis can map all potential failure modes in a system and calculate probability of failures [2, 3]. This tells designers which components are high risk.
- Reliability block diagrams simplify systems into blocks and use reliability mathematics to determine chances of failures [4]. Redundancy and backup systems can also be modeled.
- Markov chains model state changes of systems and subsystems over time [5]. The probabilities of transitioning from working to failed states can predict lifespan reliability.
- Physics-based models use mass, energy, and fluid transport balances coupled with component failures to simulate reliability [6]. Monte Carlo methods help account for uncertainties [7].
- Accelerated life testing evaluates components under exaggerated conditions to uncover failure modes missed by other methods [8].

While the discussed reliability modeling techniques provide valuable insights, they also have limitations that must be considered when analyzing intelligent regenerative life support systems:

- Individual subsystem models may not capture emergent behavior when integrated.
- Modeling assumes fixed architecture. However, systems engineering is an iterative process. Models should have opportunity for updated.

The article proposes to use the apparatus of Petri nets as a model of reliability of the class of systems under consideration. The concurrency modeling and formal analysis capabilities make Petri nets a useful reliability modeling approach for intelligent regenerative life support systems.

III. ARCHITECTURE OF LSS

Life Support Systems on board a spacecraft are critical to providing a livable and sustainable environment for the crew. This system needs to be robust and resilient, considering the isolated and extreme environment of space. The three-tiered approach includes a primary operation level, a backup system, and a reserve of consumables.

The intelligent regenerative life support system on spacecraft consists of three redundant levels designed to recycle resources and sustain human life for long-duration missions.

Level 1. The primary level contains interconnected physicochemical and biotechnological subsystems like water processors, oxygen generators, and plant growth chambers. These closed-loop reactors filter water, split water for oxygen production, and convert carbon dioxide into food and breathable air. The goal is to maximize self-sufficiency through reuse and recycling.

Level 2. Secondary backup systems provide temporary replacement capabilities using expendable supplies like oxygen tanks if the primary systems fail. This backup layer allows time for repairs and prevents catastrophic losses of critical resources.

Level 3. The third backup system is reserve consumable stocks of water, air, and food act as a buffer of last resort. These emergency reserves are sized to crew metabolic needs and mission length. They ensure survival even with prolonged primary and backup system outages.

This resilient three-tier LSS architecture allows intelligent regenerative life support systems to sustain astronauts far from Earth's resupply. The closed-loop recycling also provides insights into managing scarce resources and waste - capabilities valuable for developing sustainable habitats on Earth and beyond.

A key enabler of intelligent regenerative life support systems is the automation system (AS) that monitors conditions, controls processes, and manages failures. Without the automation system, the life support system could not maintain the closed-loop recycling and precision control needed to sustain human habitation over long durations.

The automation system comprises of networked sensors, controllers, software, and actuators. Sensors measure parameters like oxygen levels, pressure, temperature, humidity, and resource usage rates. They provide data on the current state of the life support system. The sensor data feeds into software algorithms that model the interactions of the complex ecosystem. The algorithms use techniques like feedback control, diagnostics, prognostics, optimization, and artificial intelligence to regulate the physicochemical and biotechnological processes. Actuators like valves, pumps, and switches execute the control commands that steer the system toward desired conditions.

If the automation system detects that a subsystem in the primary operation level is impaired or exhausted, it will autonomously switch to the corresponding backup system or reserve consumable to maintain continuity. This failover capability and the automation system's coordination of redundant systems is crucial for ensuring reliability.
In this case the architecture of LSS includes the next main components (Fig. 1).

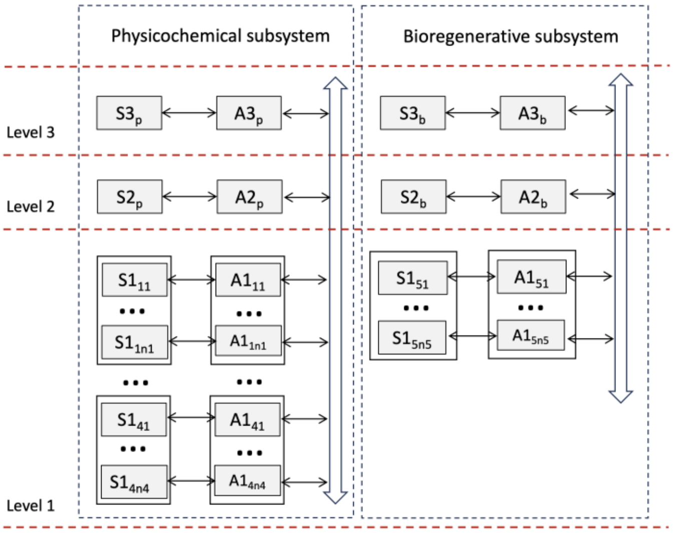


Fig.1. This resilient three-tier LSS architecture

At first level $S1_{ji}$ is j component of physicochemical subsystem with $i = 1, \dots n_j$ redundant elements, where $j = 1, \dots 5$ is number of reactor for regeneration of essential resources in closed-loop fashion: $j = 1$ - water, $j = 2$ - oxygen, $j = 3$ - methane, $j = 4$ - carbon dioxide of physicochemical subsystem and $j = 5$ - component of bioregenerative subsystem for food production. At the same first level $A1_{ji}$ is element of automation system for monitoring and control of $S1_{ji}$ LSS components.

$S2_p$ and $S3_p$ – level 2 and level 3 redundancy of physicochemical subsystem. $S2_b$ and $S3_b$ – level 2 and level 3 redundancy of bioregenerative subsystem. $A2_p$ and $A3_p$ - automation system for monitoring and control of level 2 and level 3 redundancy of physicochemical subsystem. $A2_b$ and $A3_b$ - automation system for monitoring and control of level 2 and level 3 redundancy of bioregenerative subsystem

IV. LSS DEPENDABILITY MODEL

In this study, a model based on the Petri net was used as a model for the reliability of LSS, in particular, Evaluation Petri nets, or E-nets, which are an extension of Petri nets presented in [9], seem to be especially convenient.

Petri nets offer some useful capabilities that make them well-suited for modeling the reliability of intelligent regenerative life support systems:

- Life support systems have interconnected subsystems operating simultaneously. Petri nets can model the complex sequencing and concurrency.
- Branching processes and backup systems can be modeled to analyze failure response strategies.
- Ageing and wear processes can be modeled by transition probabilities changing over time as components degrade.
- Execution of Petri net models allow system performance to be simulated over time and across failure scenarios.

The E-net can be described by set of components:

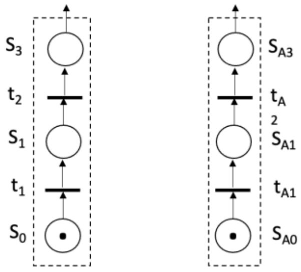
$$N = (P, T, A, M)$$

Where P is a set of places, T is a set of transitions, A is a set of arcs, M is an initial marking.

We use the method proposed in [10] for design the model based on a Petri net using typical transformation elements described in [9].

For modeling, we use a modelling element describing the occurrence of an elementary failure, shown in Fig. 2a. The main element of the simulation includes the failure generator S_0 and transition t_1 which generates initial event (defect appearance), transition t_2 which generates secondary event – appearance of failure with the law of its distribution, position S_1 and S_2 which indicate the appearance of both events.

Each LSS module has component of automation with the similar modelling element (Fig. 2b).



a) b)

Fig.2. Modelling element of elementary failure: a) LSS module; b) automation module

Using this typical element of failure development, it is possible to construct a Petri net of the entire architecture of the life support system at the highest level of complexity (Fig. 3).

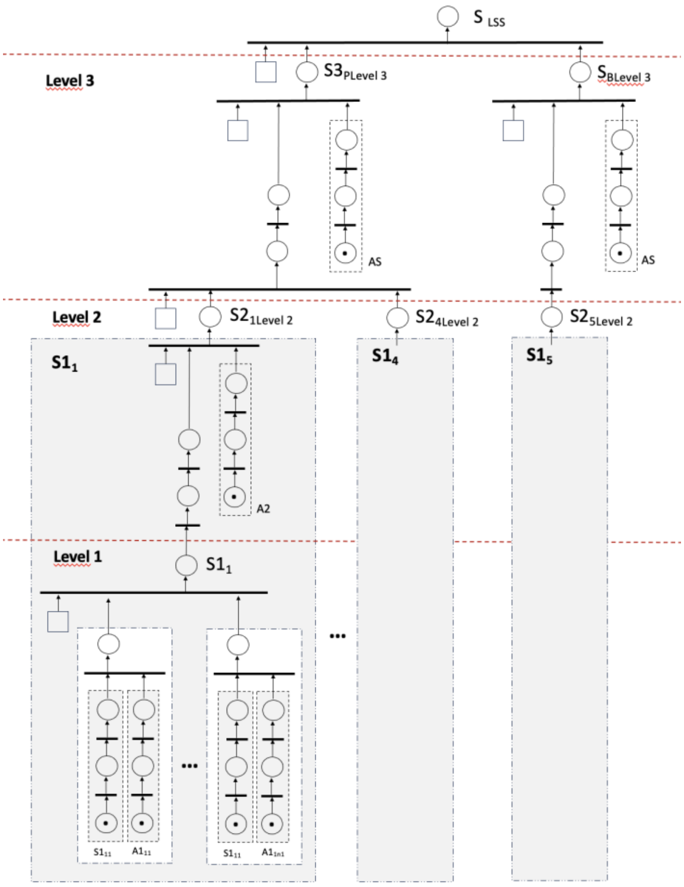


Fig. 3. Dependability model of resilient three-tier LSS architecture

The resulting model can be easily scaled in the case of a more detailed description of the individual components of the LSS architecture. Using the models of individual subsystems, obtained, for example, in [1], it is possible at the next step of detailing the model to replace the generalized models of individual LSS reactors with more detailed options. As an example, in Fig. 4 shows the transformation of the generalized reliability E-net model of the oxygen reactor to its detailed model, borrowed from [1].

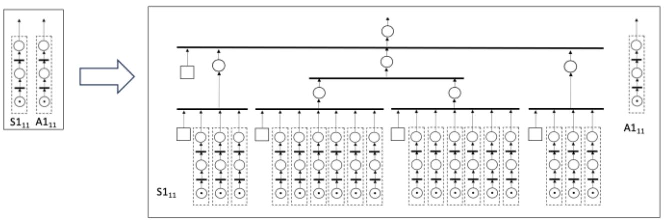


Fig. 4. Transformation of the generalized reliability E-net model of the oxygen reactor to its detailed model

Using the described methodological approach, we can propose a general algorithm and method for constructing a Petri net model for an intelligent regenerative life support system at varying levels of detail:

1. Identify key subsystems and components of the life support system architecture. These will form the basic building blocks of the Petri net model.

2. For each subsystem/component, create a generic Petri net fragment using the elementary modeling element described in the paper:

- Place S_1 models the normal working state.
- Transition t_1 models the failure event.
- Place S_2 models the failed state.
- Transition t_2 models the failure distribution.

3. Connect the subsystem fragments according to the overall system architecture to form the top-level Petri net model.

4. Simulate the top-level model to analyze overall system reliability and failure modes.

5. To add more detail, replace each generic subsystem fragment with a more specific Petri net model found in literature or developed separately.

6. Connect the detailed subsystem models to recreate the overall system model.

7. Validate that the models function correctly when integrated. Perform reliability simulations on the detailed model.

8. Iteratively add lower-level details as needed by drilling down into sub-subsystem components.

9. Use hierarchical modeling when possible, substituting macro-transitions for submodule Petri nets. This helps manage complexity.

10. Where available, use published Petri net models from literature for common components like pumps, valves, sensors, etc.

11. Carry out a computational experiment for Petri nets of various configurations using applied software [11].

V. RESULTS

The proposed Petri net modeling approach was validated through extensive simulations using the 3-tier life support system reliability model (Fig.3). The objective was assessing model performance for different failure distributions and redundancy levels.

The simulations considered exponential distribution for the first level components of LSS and the automatic switching, and logarithmic normal distribution for the second and third levels of resilient three-tier LSS architecture. The primary operating reactors (both physicochemical and biotechnological reactors) were modeled with normal distribution failures. To analyze redundancy, the primary subsystems had duplicated components.

Fig. 5 illustrates the simulation outcomes for cases with identical mean time between failures (MTBF) across all life support system (LSS) components. It varies both the MTBF value and the standard deviation of failure times for the physicochemical and biotechnological reactors.

The results demonstrate that overall LSS reliability improves markedly with increasing MTBF and decreasing standard deviation. Intuitively, enhancing component reliability and reducing variability in failure times bolsters system reliability.

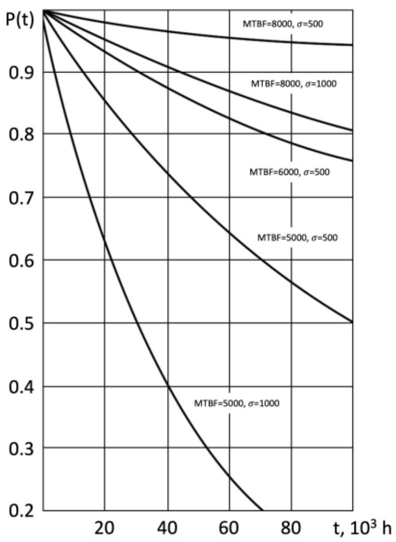


Fig.5. Dependences of the reliability function on MTBF and σ

The impacts of redundancy are shown through similar graphs of LSS reliability over time for different redundancy levels k of reactors at the primary operation level (Fig.6):

$$S1_{ij} = k \,:\, \forall i, \forall j$$

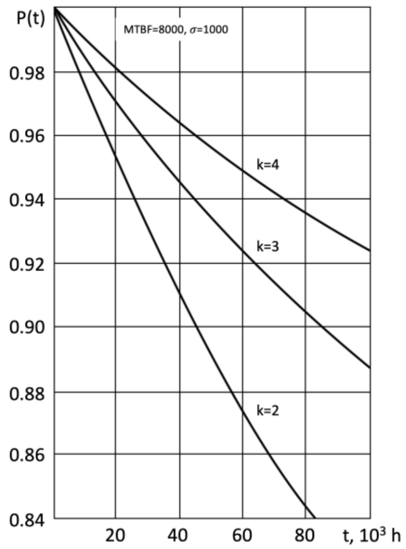


Fig. 6. Dependences of the reliability function on k

As expected, reliability grows substantially with more redundancy at this first tier.

However, the increments are nonlinear, with more modest gains as redundancy increases. This highlight diminishing returns and the need to balance redundancy versus improving individual component reliability.

The model provides valuable insights into the sensitivity of overall LSS reliability to changes in component failure parameters and redundancy. This can guide design tradeoffs when engineering these complex life support ecosystems needed for long-duration space habitation.

The model exhibits high sensitivity to subtle changes in failure parameters and distribution types of individual components. This underscores the need for rigorous subsystem reliability analysis and data to produce accurate system-level assessments. The modular architecture and hierarchical modeling approach facilitates incorporating improved subsystem models as they become available.

The decomposition into reusable modules and ability to integrate detailed subsystem models enables analysis of interactions between components that is difficult with traditional techniques like fault trees or other models. The system-level simulations capture emergent behaviors that are critical for evaluating reliability of complex intelligent life support systems with closed-loop interactions and redundancies.

VI. Discussion

The simulation showed that Petri net modeling is an advantageous technique for reliability analysis of automated regenerative life support systems. The modular methodology scales system fidelity while enabling formal analysis of crucial properties.

This research focused on development of methodological approach for modelling process on the base of E-nets. Further work should expand the technique to additional system designs, integration with other methods, software and human factors, and model optimization.

There are limitations including computational complexity for very large systems. But the demonstrated approach shows excellent promise for comprehensive reliability modeling of these safety-critical life support systems required for ambitious long-duration human spaceflight missions.

A key advantage of the Petri net modeling approach demonstrated is the ability to incorporate the effects of automation systems on overall life support system reliability. The automation system that monitors conditions, controls processes, and manages failures is a critical enabler for operation of intelligent regenerative life support systems.

The modular, hierarchical modeling methodology allows the automation system components to be represented right alongside the physicochemical and bioregenerative subsystems. This enables concurrent modeling of the complex interactions between the automation system and the processes it controls. The impacts of automation system failures on life support system reliability can be analyzed.

Unlike other reliability modeling methods like fault trees or block diagrams, Petri nets provide the capability to capture the dynamic and reactive nature of automated control systems alongside the physical processes. This facilitates evaluation of integrated, closed-loop reliable operation considering both cyber and physical components.

Analysis of life support system reliability would be incomplete without accounting for the critical automation systems. The proposed Petri net technique enables modeling these effects in addition to component failures and maintenance. This provides a more accurate picture of overall intelligent life support system dependability needed to ensure human safety on long-duration missions.

As space habitats evolve towards closed-loop ecosystems with complete recycling, developing reliable automation to control these complex systems becomes critical. Artificial intelligence promises more robust and autonomous operation, reducing dependence on humans.

There are some potential advantages of using Petri nets for modeling the AI-based automation system of a regenerative life support system:

- The concurrent nature of AI processes across distributed sensors, controllers, and actuators can be modeled effectively using Petri net semantics.
- Transitions between operating states based on sensor data, diagnostics, and control actions can be represented in the Petri net.
- Branching based on state enables modeling of AI decision logic and contingencies.
- Sensor readings can trigger key transitions between states in the model.
- Execution semantics allow modeling of real-time performance and delays.
- The automation system can be decomposed into reusable modules and layered hierarchically.
- Component wear-out over time can be represented by changing transition probabilities.
- Petri net tools allow assessment of reliability, concurrency conflicts, and response times.
- Formal verification techniques can validate logical correctness of modeled AI control logic.
- Petri nets can be modified iteratively just like the automation system's machine learning algorithms.

Petri nets provide a modeling formalism well-aligned to the distributed, concurrent, state-based, and interactive nature of intelligent automation systems. This makes them a potential fit for analyzing life support systems controlled by AI.

However, AI-based control introduces challenges in validation and verification to ensure safety. Here, Petri net modeling offers an intriguing formal method for analyzing intelligent automation systems.

Petri nets provide a mathematical modeling language well-suited for systems that are distributed, concurrent, event-driven, and interactive. This aligns well with characteristics of AI implementations typical in life support applications. Dozens of sensors and algorithms work in parallel to monitor conditions, diagnose issues, plan responses, and actuate submarine processes. Petri nets can capture the simultaneity and causal relationships between these interconnected AI components.

The Petri net transitions between discrete states also lend themselves to modeling the logic and decisions enacted by AI agents. Sensor data triggers state changes, and the model can branch based on diagnoses. This helps evaluate the AI's control logic architecturally before real-world testing. Formal verification of properties on the Petri net model then provides further confidence in the system's behavioral correctness.

In addition, Petri net simulation offers a mechanism for observing automation system performance over time and across varying scenarios. By modeling degradation and failures, one can assess the AI's responses and recovery mechanisms when disruptions occur in the life support ecosystem. This can uncover issues not evident in normal operation.

Furthermore, the modularity and hierarchy of Petri net construction allows the automation architecture to be decomposed into reusable components. This manages complexity and enables incremental modeling aligned with machine learning development cycles. Evolving AI algorithms can be represented by tweaking the Petri net structure.

For space life support systems controlled autonomously, Petri net analysis shows promise complementing other verification techniques. This rigorous modeling approach can help ensure ultra-reliable performance of intelligent automation, enabling sustainable habitats beyond Earth orbit.

This work makes important theoretical contributions in the novel modeling methodology proposed for intelligent regenerative life support systems which was not reflected in the known scientific works.

While Petri nets have been applied previously in various reliability modeling applications, their use for analyzing complex, closed-loop life support ecosystems with integrated automation are an original approach.

The modular, hierarchical modeling technique allowing seamless integration of subsystem components is a key theoretical innovation. This enables concurrent modeling of cyber-physical interactions between automation control logic and the underlying physicochemical processes not captured by traditional reliability methods. The reusable elementary failure modeling fragments and ability to substitute detailed subsystem models in a plug-and-play fashion offer scalable abstractions to manage system complexity.

Additionally, the concurrent execution modeling of distributed automation systems alongside bioregenerative processes is a theoretical advance. The proposed approach aligns well with the parallel, interactive nature of AI implementations expected in advanced life support systems. This allows architects to evaluate the impacts of intelligent automation designs on overall system reliability early in the development cycle.

The model construction methodology, modular architecture, and integrated modeling of automation alongside physical processes demonstrate important theoretical contributions uniquely suited to analysis of closed-loop, intelligent life support systems. The concepts introduced open new directions for Petri net applications in ultra-reliable cyber-physical system engineering.

The three-level life support system itself is analyzed for the first time as a single system, considering the real processes occurring during its operation from the point of view of ensuring its reliability for the end user.

Conclusion

Effective reliability modeling is imperative for designing intelligent regenerative life support systems that can safely sustain human life for long-duration space missions. This paper has proposed using Petri nets as a modeling formalism well-suited for capturing the complex concurrency and failure modes of these interconnected systems.

The three-tier architecture consisting of primary operation systems, backups, and consumable reserves was outlined. The automation system which coordinates everything was also described as a key enabler for intelligent control and failure management. A modular modeling methodology leveraging reusable component models from literature was presented. This facilitates developing hierarchical Petri net models that can scale in fidelity by substituting detailed subsystem models.

The paper demonstrated how elementary Petri net fragments can be used to represent failures and redundancy. These can be interconnected to reflect the overall system architecture. More research is still needed into integrating subsystem models while maintaining model validity as the complexity increases. Petri net analysis can verify crucial system properties and simulations assess reliability over time.

Intelligent regenerative life support systems have the potential to enable ambitious long-duration space missions by recycling resources and adapting to faults autonomously. Reliability modeling with formal methods like Petri nets complements other techniques like probabilistic risk assessment and accelerated testing. This helps ensure crew safety and mission success in the ultra-reliable way needed for human expansion into deep space.

References

[1] I. Kabashkin and S. Glukhikh, “Reliability model of bioregenerative reactor of life support system for deep space habitation,” in Dependable Computer Systems and Networks, W. Zamojski et al., Eds. Cham: Springer, pp. 105–117, 2023. doi:10.1007/978-3-031-37720-4_10

[2] X. Pan, S. Ding, W. Zhang, T. Liu, L. Wang, and L. Wang, “Probabilistic risk assessment in space launches using Bayesian network with fuzzy method,” Aerospace, vol. 9, p. 311, 2022. doi:10.3390/aerospace9060311

[3] S. Glukhikh, “Reliability model of autonomous transport with life support systems based on closed biotechnological complexes,” in Reliability and Statistics in Transportation and Communication, I. Kabashkin and I. Yatskiv, Eds. Cham: Springer, pp. 354–366, 2023. doi:10.1007/978-3-031-26655-3_33

[4] L. Carnevali, L. Ciani, A. Fantechi, G. Gori, and M. Papini, “An efficient library for reliability block diagram evaluation,” Appl. Sci., vol. 11, p. 4026, 2021. doi:10.3390/app11094026

[5] N. Bäuerle, “Markov models,” in Optimization and Operations Research, U. Derigs, Ed., vol. 4. Eolss Publishers, pp. 26–48, 2009.

[6] J. L. Garland and C. Hall, “A simple, mass balance model of carbon flow in a controlled ecological life support system,” NASA Rep., 1989. Available: https://ntrs.nasa.gov/api/citations/19900001255/downloads/19900001255.pdf

[7] K. Lange and M. Anderson, “Reliability impacts in life support architecture and technology selection,” in Proc. 42nd Int. Conf. Environmental Systems, 2012. doi:10.2514/6.2012-3491

[8] D. Wiksten and J. Swanson, “Accelerated life testing of spacecraft subsystems,” NASA TM-33-575, 1973. Available: https://core.ac.uk/download/pdf/80643877.pdf

[9] J. L. Peterson, Petri Net Theory and the Modeling of Systems. Englewood Cliffs, NJ, USA: Prentice Hall, 1981.

[10] I. Kabashkin, “Reliability model of intelligent transport systems,” in Proc. IEEE 7th Int. Conf. ITS Telecommunications, Sophia Antipolis, pp. 1–4, 2007. doi:10.1109/ITST.2007.4295911

[11] Petri Nets Tools Database. [Online]. Available: https://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/quick.html