AIAA SPACE 2008 Conference & Exposition
9 - 11 September 2008, San Diego, California

AIAA 2008-7707

Survivability and Resiliency of Spacecraft and Space-Based Networks: a Framework for Characterization and Analysis

Jean-Francois Castet[†], Joseph H. Saleh[‡]

Georgia Institute of Technology, Atlanta, Georgia 30332

Considerations of survivability and resiliency have always been of importance in the design and analysis of military systems. Over the past two decades, the importance of survivability and resiliency has expanded beyond military systems to include public networks and infrastructure systems. The analysis and assessment of networked systems with respect to survivability has become particularly acute in recent years, as attested to by a growing technical literature on the subject.

In this paper, we bring these considerations of survivability and resiliency to bear on spacecraft and space-based networks. We develop a framework for comparing the survivability and resiliency of different space architectures, namely that of a monolithic design and a distributed (or networked) space system architecture. There are multiple metrics along which different space architectures can be benchmarked and compared. We argue that if survivability and resiliency are not accounted for, then the evaluation process is likely to be biased in favor of monolithic spacecraft. We show that if in a given context survivability and resiliency are an important requirement for a particular customer, then a distributed architecture is more likely to satisfy this requirement than a monolithic spacecraft design.

We discuss in the context of our framework different classes of threats, as well as the high-frequency and low-frequency system response to (or coping strategies with) these shocks or damaging events. We illustrate the importance of this characterization for a formal definition of survivability and resiliency and a proper quantitative analysis of the subject. Finally, we propose in future work to integrate our framework with a design tool that allows the exploration of the design trade-space of distributed space architecture and show how survivability can be "optimized" or traded against other system attributes.

[†] Graduate Research Assistant, Guggenheim School of Aerospace Engineering, Student Member AIAA. Corresponding author. jcastet3@gatech.edu
[‡] Assistant Professor, Guggenheim School of Aerospace Engineering, Senior Member AIAA.

Copyright © 2008 by Jean-Francois Castet and Joseph H. Saleh. Published by the American Institute of Aeronautics and Astronautics, Inc., with permission.

I. Introduction: background on survivability and resiliency

A. Survivability and resiliency in the technical literature

SURVIVABILITY and resiliency are largely used in the scientific and technical literature as multi-disciplinary concepts in a variety of contexts and often with different meanings. A lexical search in the academic database ISI Web of Knowledge illustrates the growing frequency of the use of these concepts in the technical literature. Figure 1 summarizes the results of our literature search: the first documented use of these concepts[§] started in the 1960's with a handful of papers published on these subjects in the first decade, followed by a dramatic increase in interest in these subjects in the mid 1990's and that continues till today (over 75 papers where published on survivability in 2006 and more than 380 on resiliency). The same trend was found when the search probed for these concepts in the keywords of the publications instead of the titles. In addition, the interest in one particular topic, survivable or resilient networks, appeared in the 1980's and followed the same exponential trend (83 publications were dedicated to survivable or resilient networks in 2006).

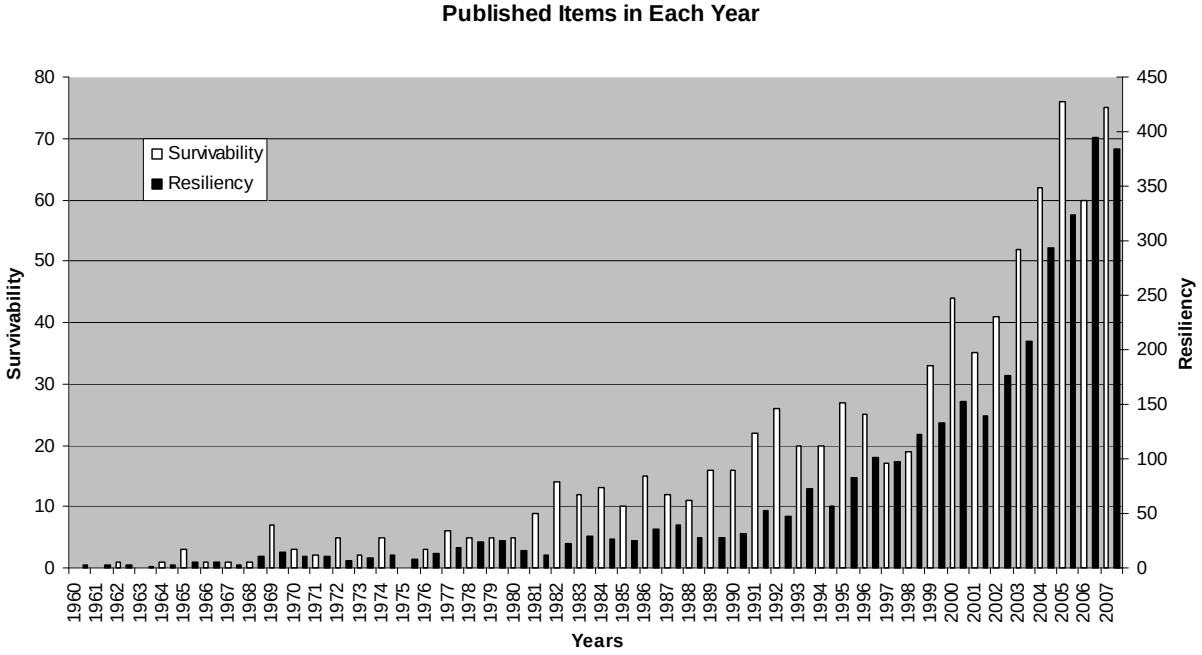

Figure 1. Survivability and resilience/resiliency publications evolution from 1960

These searches conducted on ISI Web of Knowledge also give some indication about the academic disciplines that grapple with survivability and resiliency. The concept of survivability is traditionally associated with engineering whereas resiliency is more often found and discussed in environmental sciences as well as in psychology and psychiatry. Note that the words resilience or resiliency can be equally found in papers, with no difference in meaning. As a consequence, only the word resiliency will be used in this paper.

[§] Used in the titles of technical publications.

B. Survivability concept

1. Military context

Survivability has become increasingly important since the 1960's [1] as a strategic concept for the military. It is applied to platforms (e.g. aircraft), people, systems (e.g. military network), and now more generally to missions.

Several papers show this evolution, from one of the first attempts to assess survivability linked to an aircraft in 1967 [1, 2] to some more general definitions [3, 4, 5, 6] as the one provided by the DoD Regulation 5000.2-R [6]: "[survivability is] the capability of a system and crew to avoid or withstand a man-made hostile environment without sustaining an impairment of its ability to accomplish its designated mission. Survivability consists of susceptibility, vulnerability, and recoverability." Susceptibility is "the degree to which a weapon system is open to effective attack because of one or more inherent weakness"; vulnerability is "the characteristic of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having being subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment"; recoverability is "the ability, following combat damage, to take emergency action to prevent the loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities"

Several publications have addressed the issue of survivability of military networks, a growing field since the 1980's and 1990's [7], defining survivability of a military network as the "ability to maintain communication among the nodes when it is subject to deliberate destruction".

2. Engineering context

During the past two decades, the concept of survivability has spread over other areas than the military, especially to electrical and electronic engineering with an emphasis on software, telecommunications, and information systems. In particular, survivability has become of major interest for network systems designers since society has become significantly dependent on a variety of networks, leading to severe consequences in the case of network system disruptions or failures.

While the use of survivability is widespread within the technical and scientific community, no definition is unanimously adopted. Westmark (2004) [8] compiled 53 definitions of survivability from different papers to provide a definition template: survivability, according to Westmark, is "the ability of a given system with a given intended usage to provide a pre-specified minimum level of service in the event of one or more pre-specified threats". Present in Westmark's list, one of the more cited definitions is provided by Ellison (1999) [9]: survivability according to Ellison is the "capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents". Knight (2003) [10], while also providing survivability definitions in the telecommunications and software field, found this definition not precise and formal enough. Knight attempts to provide a formal definition of survivability based on six quantitative parameters (or sextuple). He characterizes a system as "survivable if it complies with its survivability specification," and the survivability specification is mathematically defined, gathering all acceptable levels of service from the system, the associated services values and relative values (perceived by the user), its probabilistic requirements and its possible transitions in a specified operating environment.

Accordingly, survivability definitions teeter between informal and formal definitions, and occasionally, but not always, survivability is defined in probabilistic terms. But, as observed from the previous definitions, survivability is context-specific, related to the system studied, its environment, and the services and requirements the user has chosen. This specificity explains why often survivability seems to be a more generic word defined or measured in terms of other notions, like availability, performance, security, reliability, traffic capacity, connectivity, etc. However, contrary to reliability linked to normal environment, survivability is related to the system response with respect to abnormal conditions.

Also, note that the existing definitions sometimes include different concepts, and particularly the notion of recovery, recoverability or restoration. In some papers, recovery is a subset of survivability, whereas in others, survivability is limited to the behavior of the system during the abnormal conditions without time consideration.

C. Resiliency concept

Resilience or resiliency is also a concept with multiple definitions. As explained in Caralli (2006) [11], resiliency was first used to describe a property of a physical material. It is "the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress" according to the Merriam-Webster Dictionary. Resiliency has expanded beyond this physical definition to other disciplines and particularly in ecology [12] and psychology where "resiliency refers to the ability of people to bounce back from adversity" [11]. It is now applied also to engineered networks and organizations.

However, despite the diversity of disciplines interested in resiliency, three elements are present across most definitions according to Caralli: the ability to "change when a force is enacted, [to] perform adequately or minimally while the force is in effect, [to] return to a predefined expected normal state whenever the forces relents or is rendered ineffective". Thus time becomes an important parameter in resiliency estimation, accounting for the whole system response, from the shock to the after-shock. Finally, resiliency is an emergent property of the system, i.e. resiliency is a property of the system as a whole, at a macroscopic scale.

D. Resiliency versus survivability

Survivability and resiliency have been compared in several papers due to their close nature. According to the ResiliNets Initiative [13], resiliency is the "ability of the network to provide and maintain an acceptable level of service in the face of various challenges to normal operations". Resiliency is considered "as survivability plus the ability to tolerate unusual but legitimate traffic load". Consequently, resiliency is seen as a superset of survivability.

Other papers considered also resiliency as a superset of survivability, but in another respect, perhaps more relevant: Caralli (2006) [11] views resiliency as an extension of survivability (which deals only with the shock) to include "risk prevention as well as restoration of normal processes once a disruption has relented". Time dependency is included in the definition of resiliency and a system will be said resilient, with respect to a threat and a service, considering its response before, during and after the abnormal condition(s). In the following, our definition will be based on the definition from Caralli.

E. Survivability and resiliency models

Several models have been proposed to compute survivability of various systems. Westmark (2004) [8] provides an extensive literature review of these models. Different models to compute survivability or resiliency are used, such as state machines, trellis graphs, Markov processes, Monte Carlo simulations, topology of networks, etc. No particular trend can be attributed to each considered field. As for the definitions survivability or resiliency, no model is unanimously adopted.

II. Survivability and resiliency definitions – System response

Contrary to reliability, survivability deals with degraded states of performance. Indeed, reliability is only a binary concept, where the system is either fully operational, or failed under normal operations. Survivability allows a great level of precision in describing the system's performance degradation facing abnormal conditions.

As stated before, survivability is defined in a certain environment, with respect to threat(s) and a performance index chosen by the user to assess the performance of the system considered. As this definition is context-specific, the environment, the threat(s), the performance index will have to be specified each time an analysis is conducted. Figure 2 illustrates the system response facing a shock. The survivability of the system is computed with the performance degradation ΔP. Note that survivability deals only with the immediate reaction of the system at the shock, and can thus be conceived of as the high frequency response of the system to the shock. On a side note, particularly desirable for high-availability systems such as communications satellites, graceful degradation allows the system to keep operating and continues to provide some services by staging its performance degradation over time.

The response of the system after the shock is captured by the recoverability of the system, which in simple terms can be thought of as a time parameter τ modeling the necessary time for the system to return within a certain

percentage of the initial level of performance (e.g. 95% response). Here again, recoverability can be conceived of as the low frequency system response to a shock.

Resiliency is defined in this paper as the superset combining survivability and recoverability.

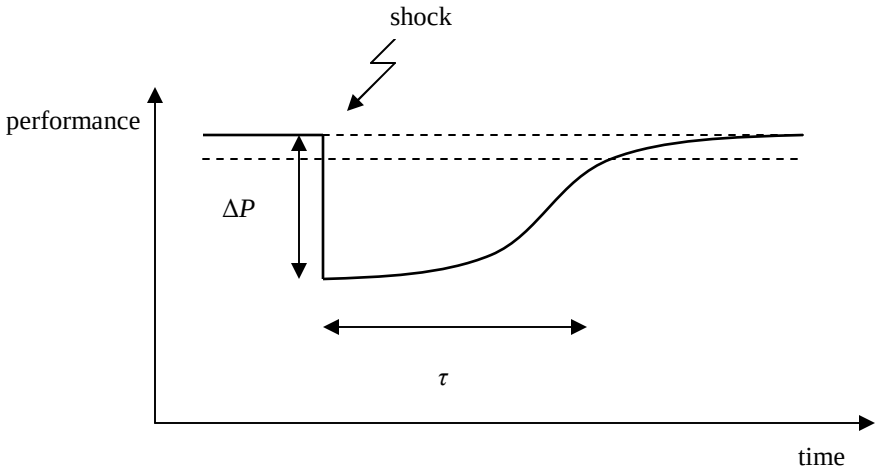

Figure 2. System response during and following a shock

III. Survivability framework

A. Presentation

According to the previous definitions, we want to assess and compare the survivability of spacecraft and space-based networks, facing threats and with respect to some performance measures. We call a co-located space-based network a cluster of satellites having the capability of communicating between each other, and thus being able to share resources. For example, the mission data processor (MDP) can be divided between several satellites, these MDPs collaborating to fulfill the function, or some small MDP acting as a back-up of the main processor located on one satellite of the network.

This paper addresses survivability considerations; resiliency will be treated in future work. We develop in this paper an analytical model that assesses the survivability of a system, as shown in Figure 3.

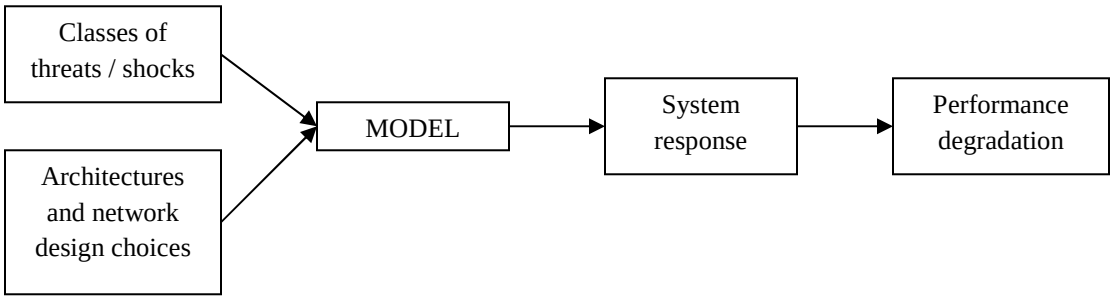

Figure 3. Framework presentation

As a first step to demonstrate the capability of our model, we limit the scope of this study to the following particular case: the shocks considered are the on-orbit failures actually observed in the satellite subsystems (i.e.,

actual field data). Two types of space system architectures are considered in this work: the traditional monolith spacecraft and a co-located space-based network. From the obtained performance degradation, the survivability of the two architectures is compared.

B. Statistical data analysis and hazard rate modeling

The stochastic laws modeling the degradation of each subsystem were deduced in previous works by Castet and Saleh (2008a, 2008b) [14, 15]: from the SpaceTrak® database [16], a statistical analysis was conducted to determine the distribution hazard rates of the satellite and its subsystems. Due to the censored nature of the sample composed of 1745 satellites and about 870 associated anomalies or failures, a Kaplan-Meier estimator was used to obtain estimated reliability functions of satellites or subsystems, as well as estimated probabilities of transition between degraded states. Weibull distributions were chosen to fit the Kaplan plots representing the empirical data, due to the flexible nature of the Weibull distribution to model time-dependent hazard rates. Weibull distributions resulted in excellent fit with the empirical data.

In space-based networks, the different spacecraft can be composed of possible different subsystems. Thus there is a real necessity of obtaining reliability and probability data at a subsystem level. From the database, 13 subsystems were considered:

- Attitude control
  - Gyro/Sensor/Reaction wheel
  - Ion/Electric thruster
  - Thruster/Fuel
- Beam/Antenna operation/deployment
- Control Processor
- Mechanisms/Structures/Thermal
- Payload Instrument/Amplifier/On-board data/Computer/Transponder
- Power
  - Battery/Cell
  - Electrical distribution
  - Solar Array Deployment
  - Solar Array Operating
- Telemetry Tracking and Command
- Unknown

Several degraded states were considered at a subsystem level: 4 anomaly event classes described in the following.

- **Class I**: satellite retirement due to subsystem failure
- **Class II**: major non-repairable failure that affects the operation of a satellite or its subsystem on a permanent basis
- **Class III**: major non-repairable failure that causes the loss of redundancy to the operation of a satellite or its subsystems on a permanent basis
- **Class IV**: minor/temporary/repairable failure

From these subsystems and anomaly event classes, 54 Weibull hazard rate models were developed according to the technique described above. These models are part of a multi-state failure analysis conducted previously by the authors (Castet and Saleh, 2008b) [15].

C. Stochastic Petri Net

Our model uses Stochastic Petri Nets (SPNs). Invented in 1962 by C. A. Petri, a Petri net is a mathematical representation of a discrete distributed system (concurrent processes). A Petri net is composed of tokens (relevant entities of the system), places (possible states of the entity), transitions (rules for token movements) and arcs (links between places and transitions). The combination of the locations of the tokens, called the marking, uniquely characterizes the state of the system. SPNs compose a subfamily of the Petri nets, adding a stochastic behavior through adjustable randomness of the transitions (exponential, Weibull, normal, lognormal… distributions). The reader is referred to Haas [17] for additional details on stochastic Petri nets. Figure 4 provides an illustrative example of a SPN.

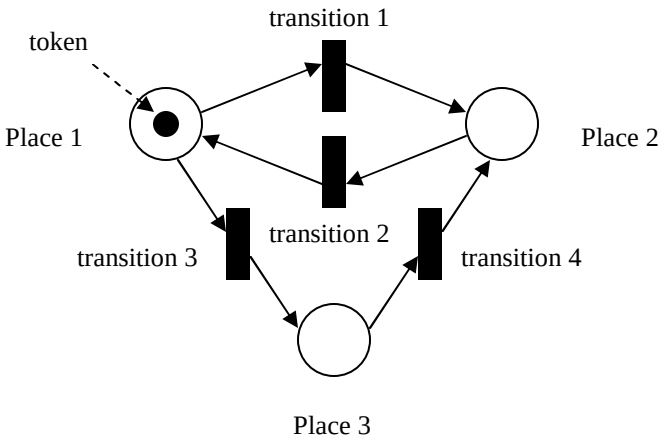

Figure 4. Example of a stochastic Petri net

Two particular arcs are used in the model: inhibitor arc and enabler arc. An inhibitor arc prevents a transition from firing when a token is present in the place linking the transition and the place. An enabler enables the transition contrary to an inhibitor, as presented by Volovoi (2006) [18]. Examples of an inhibitor and enabler are presented in Figures 5a and 5b.

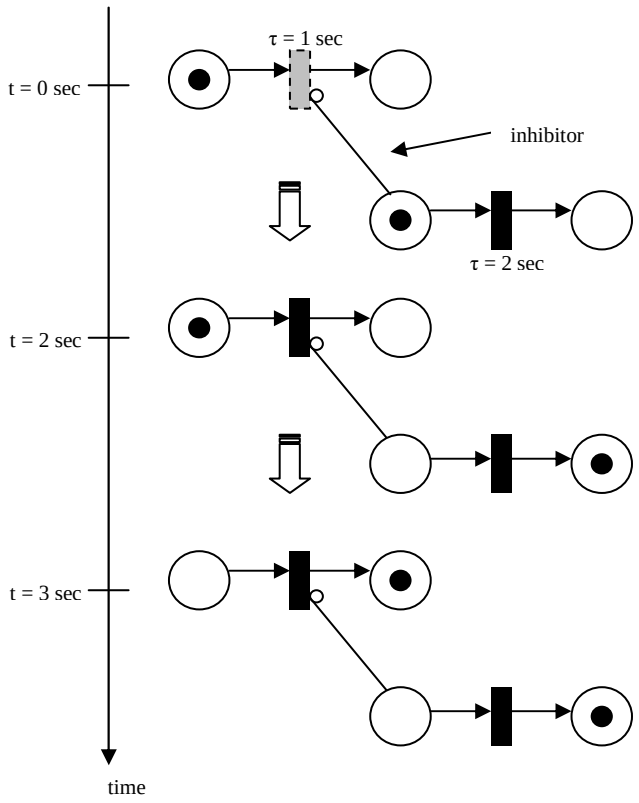

Figure 5a. Example of an inhibitor

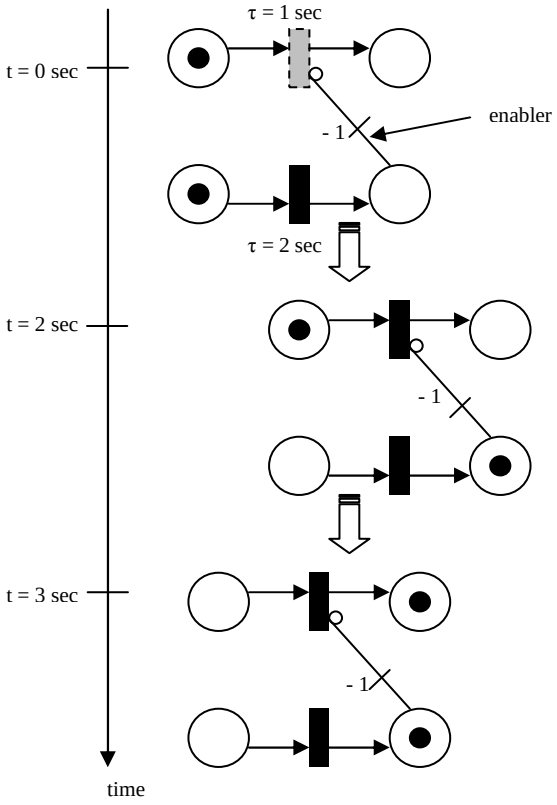

Figure 5b. Example of an enabler

In Figure 5a, we can see the evolution of the system including an inhibitor: even if the upper transition is faster than the lower one, the presence of a token activating the inhibitor at the initial time prevents the upper transition to fire after 1 sec. The lower transition fires after 2 sec, deactivating the inhibitor and enabling the upper transition which fires one second later. Figure 5b models the same system behavior with an enabler: the upper transition is activated by the enabler after the 2 sec needed by the lower transition to fire.

We choose SPNs as our analytical and modeling tool over Markov Chains (MCs), because 1) stochastic Petri nets allow local modeling unlike Markov Chains which are confined to a global approach, and 2) time dependencies and local clocks are much more easily implemented in stochastic Petri nets than in Markov Chains. Local analysis is important in our study to model the interaction between satellite subsystems and system levels. Time dependency is needed to model the evolution of satellite subsystems hazard rates through time (no constant hazard rates as seen before). However, because of the local nature of SPNs, Monte Carlo simulations are necessary to generate a representative behavior of the stochastic transitions. Due to the complexity of our SPN models described in the following, one million runs were conducted with each model to obtain an acceptable level of precision.

D. Model

Four states were considered at the system level:

- operational: 0 – 5% performance loss
- minor degradation: 5 – 35% performance loss
- major degradation: 35 – 85% performance loss
- failed: 85 – 100% performance loss

These states generate the survivability level of precision of our model. The probabilities of being in these four states are the output of the SPN model. Comparisons between the probabilities obtained for each of the two architectures allow a survivability analysis of the architectures considered.

In the case of a monolith architecture, the following rules are used to link the subsystem and system levels:

- the system is in the operational state if all the subsystems are in their operational states
- the system is in the failed state if one subsystem is in Class I state
- the Class IV and Class III state of the subsystems do not have a direct effect on the system level
- the Class II state can lead to minor, major degradation or failed system states according to probabilities peculiar to each subsystem

According to the stochastic laws inferred for each subsystem as Weibull distribution hazard rates and the previous rules, a stochastic Petri net model is developed to model a monolith satellite facing on-orbit failures and anomalies. Figure 6 presents this model.

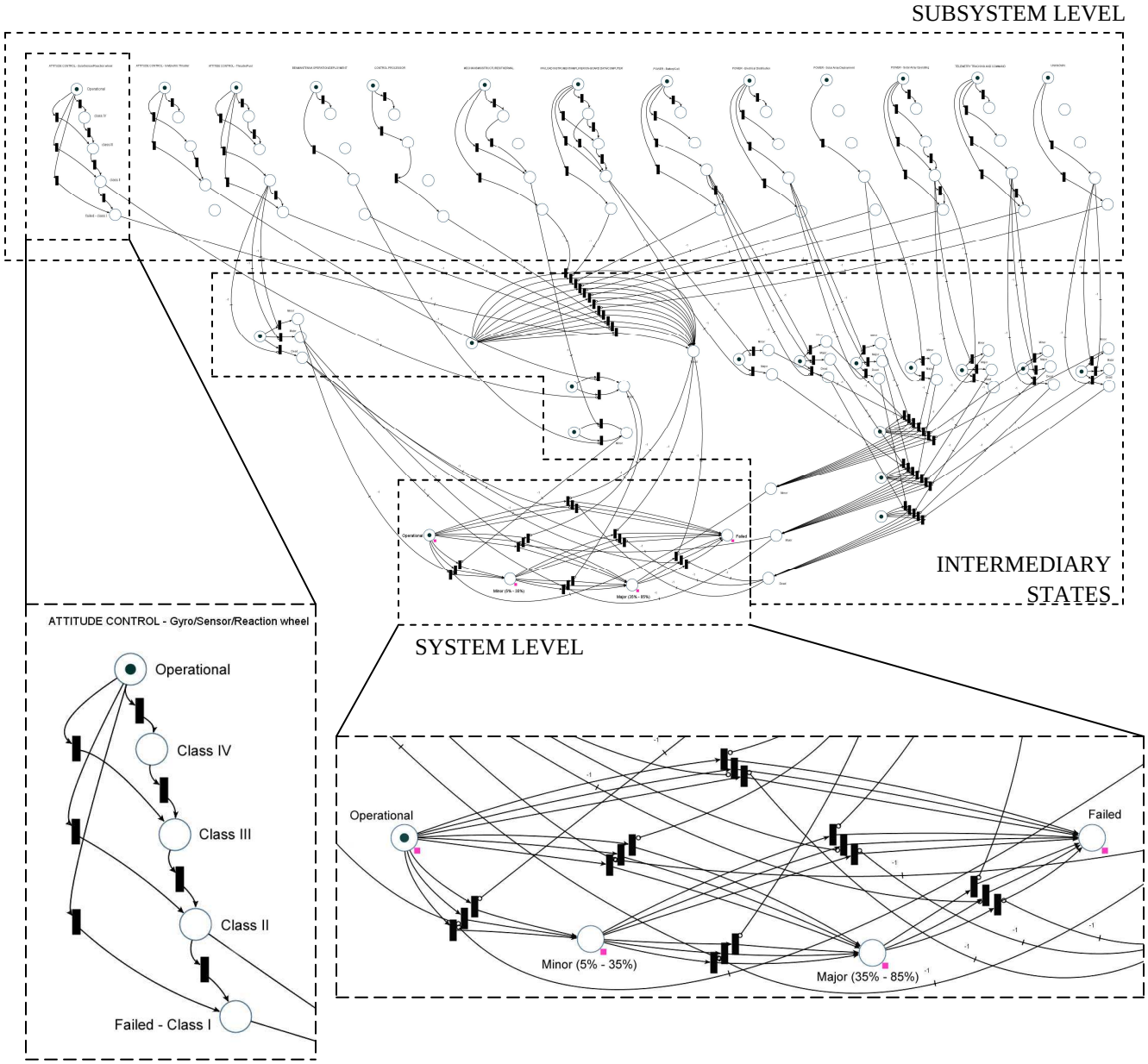

Figure 6. SPN model of a monolith spacecraft: multi-state failure model linking subsystems failures to system failures

Concerning the co-located space-based network architecture, a particular case is chosen as a demonstration for the developed SPN tool: two networked spacecraft are considered, the first one containing all the 13 subsystems (i.e. a monolith one with the ability to talk to other satellites; we call BOX1 all the subsystems but the Telemetry Tracking and Command (TTC) subsystem), the second having the necessary subsystems for a satellite (called here BOX2: attitude control, power, antenna and mechanism/structures/thermal) plus a TTC subsystem acting as a single TTC "redundancy". Indeed we want to observe the effects of a spacecraft having the ability to tap into the resources of another one in case of the damage of its own subsystems. Some rules are also used to link subsystem to system level:

- System Failed:
  - If BOX1 Failed
  - If TTC1 Failed & TTC2 Failed
    or BOX2 Failed

- System Major:
  - If BOX1 Major
  - If TTC1 Failed & TTC2 Major
  - If TTC1 Major & TTC2 Failed
    or TTC2 Major
    or BOX2 Failed
- System Minor:
  - If BOX1 Minor
  - If TTC1 Minor & TTC2 Minor

Figure 7 presents the SPN model for the co-located space-based network architecture, BOX1 and TTC1 constituting the first spacecraft while BOX2 and TTC2 constituting the second spacecraft.

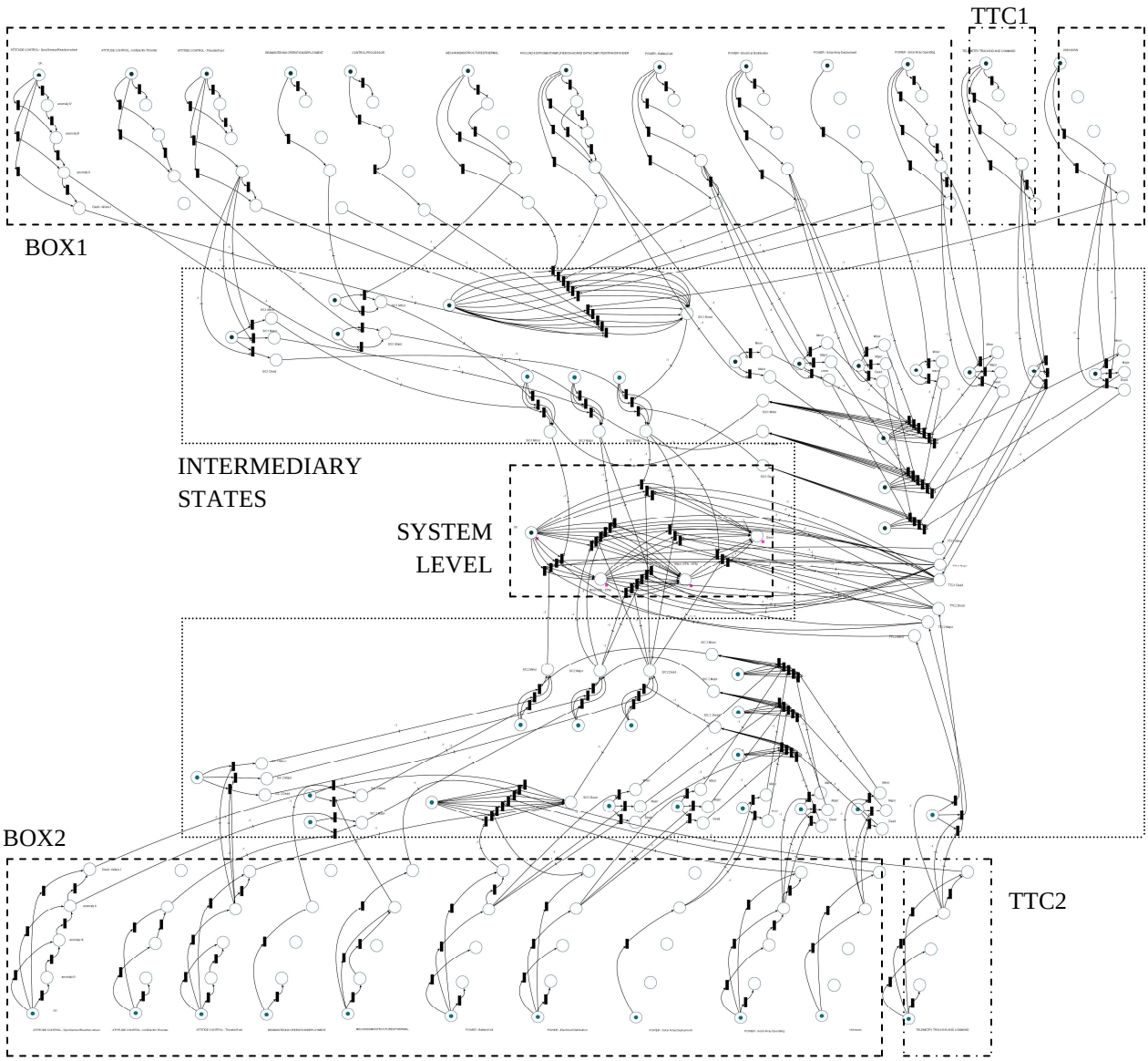

Figure 7. SPN model of a co-located space-based network architecture: multi-state failure model linking subsystems failures to system failures

E. Validation

Validating partially the model is done by evaluating the monolith reliability, by multiplying the probabilities of being in the Class I state for the 13 subsystems in the SPN model. Figure 8 presents the comparison between the original Kaplan-Meier estimated satellite reliability to the reliability given by the SPN model. The SPN model output closely approximates the spacecraft reliability field data (or more precisely the Kaplan-Meier estimate of the spacecraft reliability based on the censored field data). The SPN model output is significantly accurate over the first eight years of spacecraft operation, and remains within 1% of the field data over 16 years.

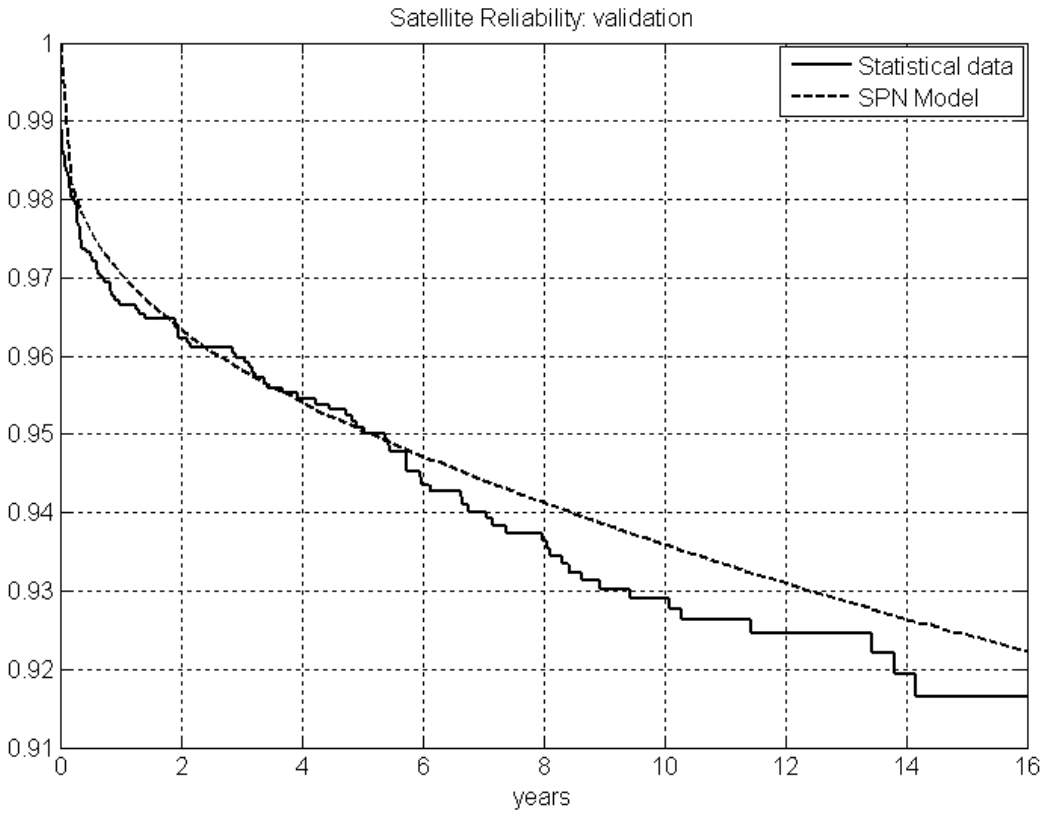

Figure 8. Comparison between statistical data and SPN model

F. Results

1. Monolith architecture

Running the Monte Carlo simulation of the SPN model in the case of a monolith architecture provides the evolution in time of the probabilities of the system being in operational or different failed states (i.e., operational, minor and major degradation, failed). Figure 9 presents these results.

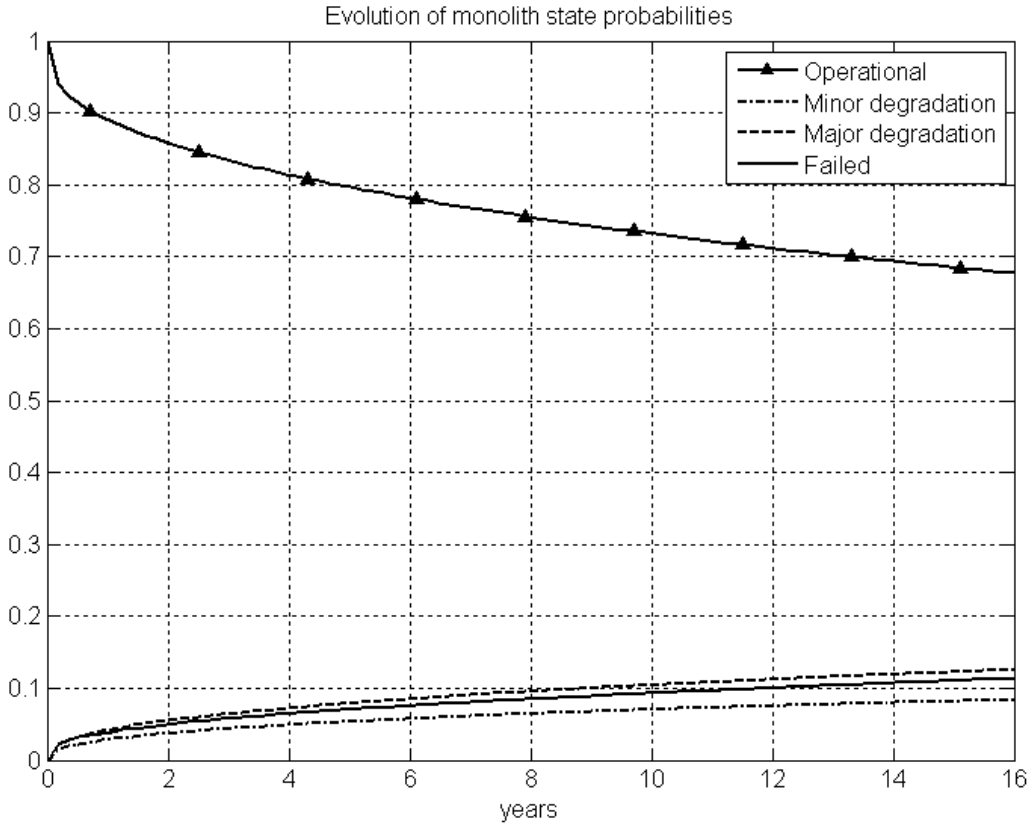

Figure 9. State probabilities results in the case of a monolith architecture

Figure 9 reads as follows: consider for example a monolith spacecraft after six years on-orbit. It has a 78% likelihood of being fully operational, 6% of being in minor degradation, 8.5% of being in major degradation and 7.5% of being in a failed state. The probability of being fully operational decrease quickly the first year (while the probability of being in the other states increase quickly) and at a slower rate on the following years.

Note that even if the x-axis is the time, the studied notion stays survivability. Each point in the plot gives a probability of the magnitude of the degradation of the performance ΔP any time. Recall there are no repairs, maintenance policies or recoverability involved in this analysis.

2. Space-based network architecture and survivability comparison of the two architectures

Running the same simulation for a co-located space-based architecture leads to the same kind of plots. Figures 10a and 10b present two of the four plots resulting to the comparison between the two architectures for the operational and the failed states.

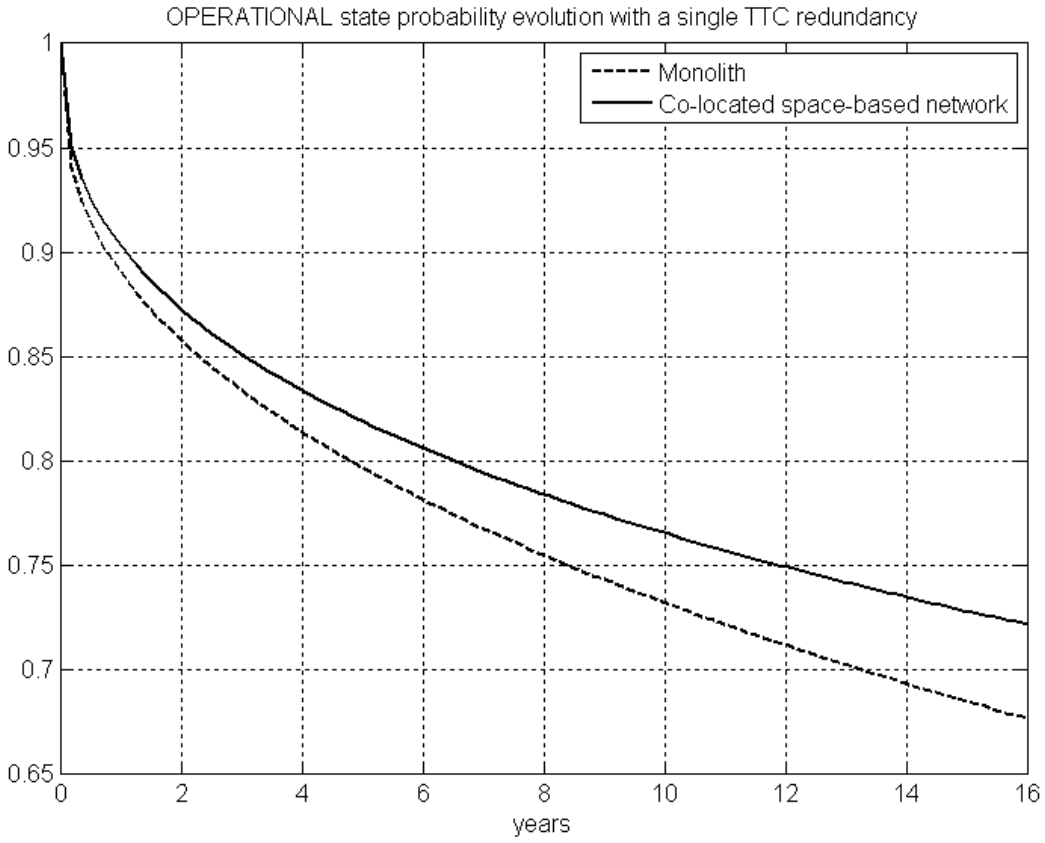

Figure 10a. Comparison between monolith and co-located space-based architectures for the operational state

Figure 10a is confined to the operational state and clearly shows that the co-located space-based network gives better results at any point time than the monolith spacecraft: in simple terms, a co-located space-based network is more likely to remain (or be found) in an operational state than the traditional monolithic spacecraft. The following Figure 10b shows the result for the failed state. A more precise analysis of these results is provided shortly, following Figure 11, which presents a more exhaustive and compact comparison between the two architectures.

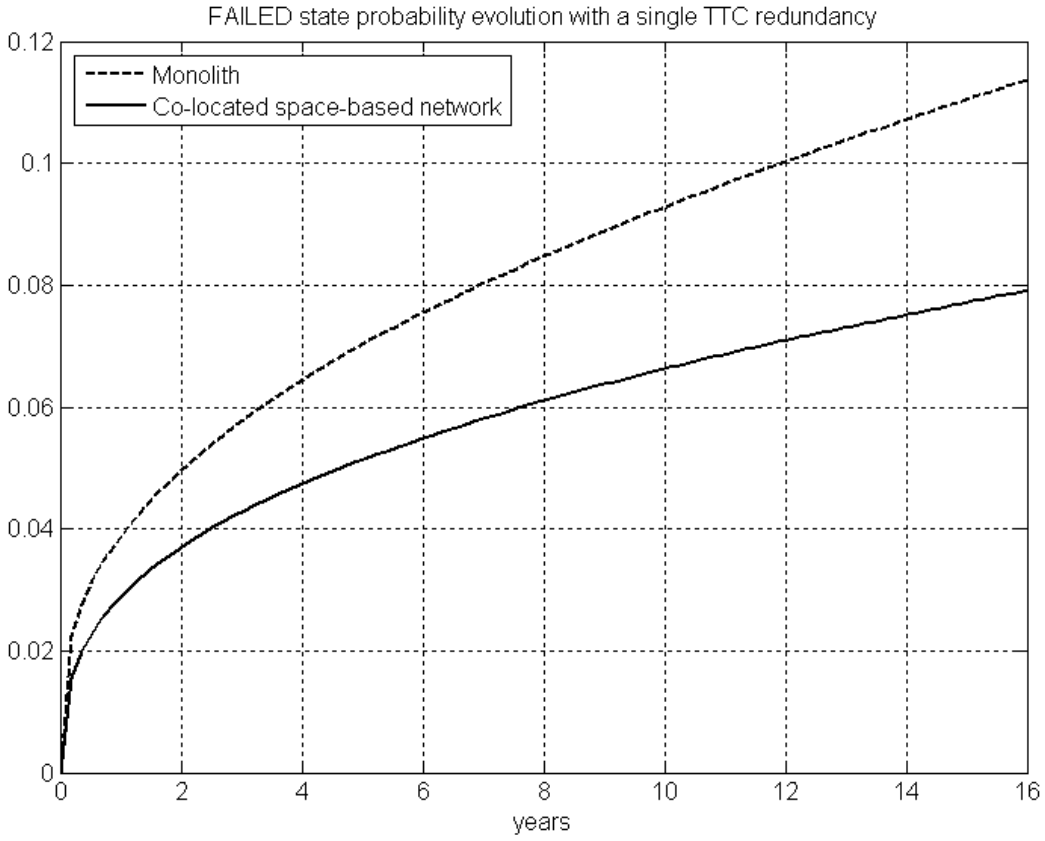

Figure 10b. Comparison between monolith and co-located space-based architectures for the failed state

Here again, the advantage of the two-networked satellite architecture is clear: a co-located space-based network is less likely to be in a failed state than the traditional monolithic spacecraft. The four plots are combined in one as shown in Figure 11: the figure represents the difference in the resulting probabilities of being in any of the fours states between the two architectures. The y-axis is the difference in percentage point between the two architectures.

- For the operational state, the difference is positive: the probability of being in an operational state is higher at any point in time for a co-located space-based network than for a monolith spacecraft. In particular, it is greater by about 4.5% after 16 years, that is, instead of having 67.5% likelihood of being in an operational state after 16 years of operation for the traditional monolithic architecture, the networked architecture has a 72% likelihood of being in an operational state. Note that this additional probability of remaining in an operational state can be of significant importance to the owner of the system or end-users of the services provided by the system.
- For the minor, major degradation and failed states, the difference is negative, meaning that the probabilities to be in these states are lower for a co-located space-based network than for a monolith one, with a bigger difference for the failed state (about 3.5% less after 16 years). The same interpretation as in the previous bullet point applies as well in these cases.

Consequently, the co-located space-based network architecture is more survivable than the monolith spacecraft at any time in this context, i.e., with respect to TTC failure. No other more general conclusion on the survivability of a co-located space-based network architecture can be inferred from this demonstration study.

Note that in this context, the difference in state probabilities between the two architectures increase with time, that is, the co-located space-based network becomes increasingly more survivable with time compared with the monolithic spacecraft.

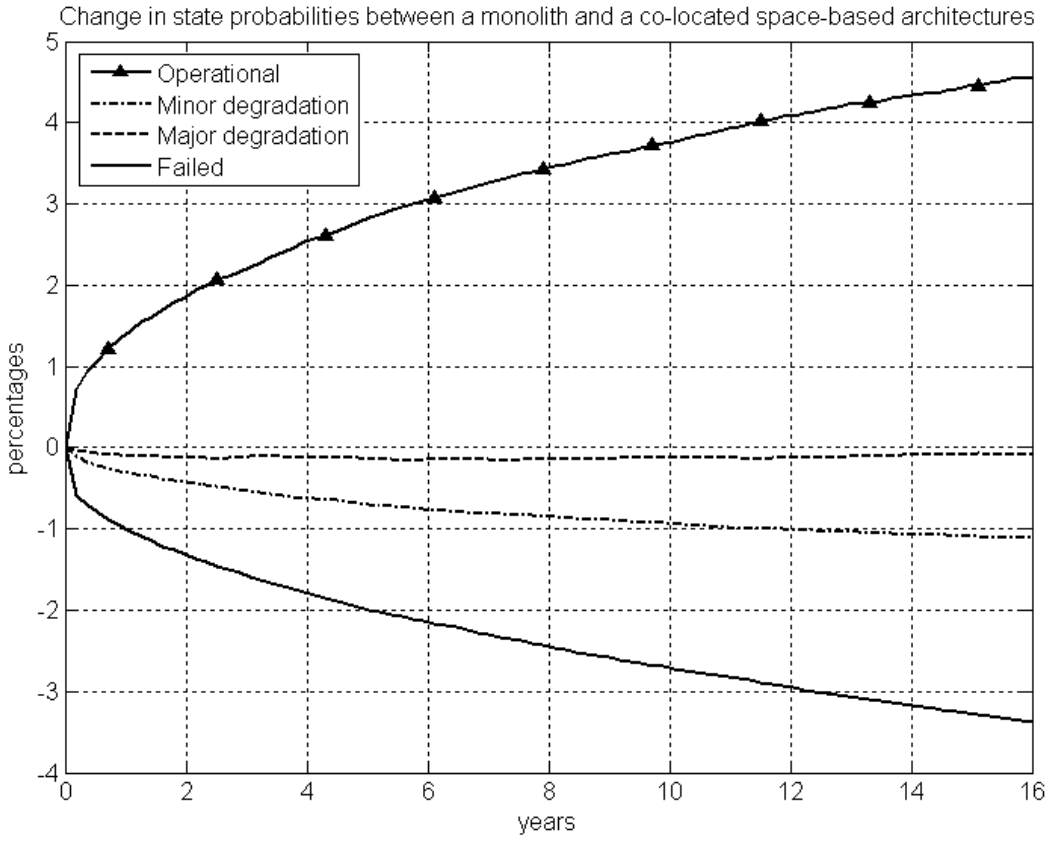

Figure 11. Survivability superiority of the co-located space-based architecture over a monolith

IV. Conclusion

In this paper, we first provided a literature review on survivability and resiliency, showing that despite the increasing popularity of the two concepts, no definitions or models are unanimously adopted within the technical and scientific community. Assimilated to high and low frequency response of the system facing a shock, survivability and resiliency are defined according to the specific context of a given study, including the system's environment, threats, user services and performance measures.

Following our literature review, we developed a survivability tool for space systems using stochastic Petri nets. In the case of on-orbit failures, the SPN transition laws are based on actual satellite subsystems hazard rates given by a statistical lifetime data analysis (Kaplan-Meier estimator). We chose a particular configuration of a co-located space-based network to demonstrate the capability of the tool, using Monte Carlo simulations to generate representative results of stochastic behavior of the spacecraft on-orbit anomalies and failures. A comparison between the two architectures leads to the conclusion that in the context and configuration we have chosen, the co-located space-based network is more survivable than the traditional monolith spacecraft. In other words, if in a given context survivability is an important requirement for a particular customer or end-user of a space asset, then a networked space-based architecture is more likely to satisfy this requirement than a traditional monolithic spacecraft. This observation has important implications for the design and acquisition of space systems. Consider the following: there are multiple metrics along which different proposed space system designs are benchmarked and compared, cost being one important factor. It is likely that a networked space-based architecture will incur a cost penalty compared with a monolithic spacecraft, even on an iso-performance basis. Therefore if one of the advantages of a

space-based network, namely its survivability, is not accounted for, then the evaluation process is likely to be biased in favor of the monolithic spacecraft (on a cost basis).

In future work, we propose to further develop and integrate our survivability tool with a space system design trade-space exploration tool. In addition, we propose to add resiliency considerations while accounting for repair and replacement (maintenance) policies.

Acknowledgments

This work was funded in part by a grant from OSC/DARPA from the F6 program. Their support is gratefully acknowledged.

References

[1] Ball, R.E., Atkinson, D. B., "A History of the Survivability Design of Military Aircraft", AIAA-1995-1421, *AIAA/ASME/ASCE/AHS/ASC, Structures, Structural Dynamics and Material Conference, 36th*, New Orleans, LA, April 10-12, 1995.

[2] Atkinson, D. B., Blatt, P., et al., "Design of Fighter Aircraft for Combat Survivability", Paper 690706, Society of Automotive Engineers, National Aeronautic and Space Engineering and Manufacturing Meeting, Los Angeles, California, Oct. 6-10, 1969.

[3] MIL-STD-2069, *Military Standard Requirements for Aircraft Nonnuclear Survivability Program*, 24 August 1981.

[4] MIL-HDBK-2069, *Military Handbook, Aircraft Survivability*, 10 April 1997.

[5] MIL-HDBK-336-1, *Military Handbook, Survivability, Aircraft, Nonnuclear, General Criteria*, Vol. 1, 25 October 1982.

[6] DoD Regulation 5000.2-R, 'Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs", 11 May 1999.

[7] Haizhuang Kang, Butler, C., Qingping Yang, Jiamo Chen, "A New Survivability Measure for Military Communication Networks", *Military Communications Conference*, Vol. 1, IEEE, 1998, pp. 3-4.

[8] Westmark, V. R., "A Definition for Information System Survivability", *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 5-8 Jan. 2004.

[9] Ellison, B., Fisher D. A., Linger, R. C., Lipson, H. F., Longstaff, T., Mead, N. R., "Survivable Network Systems: An Emerging Discipline", SEI, May 1999 (1997 revised version).

[10] Knight, J. C., Strunk, E. A., Sullivan, K. J., "Towards a Rigorous Definition of Information System Survivability", *Proceedings of DARPA Information Survivability Conference and Exposition, 2003*, Volume 1, 22-24 April 2003, pp 78-89.

[11] Caralli, R. A., "Sustaining Operational Resiliency: A Process Improvement Approach to Security Management", Carnegie-Mellon University, Pittsburgh, PA, Software Engineering Institution, 2006.

[12] Walker, B., Holling, C.S., Carpenter, S. R., Kinzig, A., "Resilience, adaptability and transformability in social–ecological systems", *Ecology and Society*, Vol. 9, No. 2, Art. 5, 2004. [online] URL: http://www.ecologyandsociety.org/vol9/iss2/art5/.

[13] Xie, L., Smith, P., Banfield, M., Leopold, H., Sterbenz, J. P.G., Hutchison, D., "Towards Resilient Networks using Programmable Networking Technologies", *Seventh Annual International Working Conference on Active and Programmable Networks (IWAN 2005)*, Sophia Antipolis, France, November 2005.

[14] Castet, J. F., Saleh, J. H. (2008a) "Satellite Reliability: Updated Historical Data, Statistical Analysis and Weibull Modeling" submitted to the Journal of Spacecraft and Rockets, 2008.

[15] Castet, J. F., Saleh, J. H. (2008b) "Multi-state Failure Analysis of Spacecraft and Spacecraft Subsystems: Statistical Data Analysis and Modeling" submitted to Reliability Engineering and System Safety, 2008.

[16] Ascend SpaceTrak® [online database], URL: http://www.ascendworldwide.com/spacetrak.aspx [cited 1 July 2008].

[17] Haas, P., *Stochastic Petri Nets: Modelling, Stability, Simulation*, Springer-Verlag, New York, 2002.

[18] Volovoi, V., "Stochastic Petri Nets Modeling Using SPN@", *RAMS-2006 Symposium*, Newport Beach, CA, January 26-29, 2006; Paper 2006RM-166.