Reliability Engineering and System Safety 99 (2012) 123–138

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

On the concept of survivability, with application to spacecraft and space-based networks ☆

Jean-Francois Castet, Joseph H. Saleh *

Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Article history:
Received 17 January 2010
Received in revised form
21 November 2011
Accepted 23 November 2011
Available online 9 December 2011

Keywords:
Survivability
Multi-state failure
Spacecraft
Space-based network
Stochastic Petri net

ABSTRACT

Survivability is an important attribute and requirement for military systems. Recently, survivability has become increasingly important for public infrastructure systems as well. In this work, we bring considerations of survivability to bear on space systems. We develop a conceptual framework and quantitative analyses based on stochastic Petri nets (SPN) to characterize and compare the survivability of different space architectures. The architectures here considered are a monolith spacecraft and a space-based network. To build the stochastic Petri net models for the degradations and failures of these two architectures, we conducted statistical analyses of historical multi-state failure data of spacecraft subsystems, and we assembled these subsystems, and their SPN models, in ways to create our monolith and networked systems. Preliminary results indicate, and quantify the extent to which, a space-based network is more survivable than the monolith spacecraft with respect to on-orbit anomalies and failures.

For space systems, during the design and acquisition process, different architectures are benchmarked against several metrics; we argue that if survivability is not accounted for, then the evaluation process is likely to be biased in favor of the traditional dominant design, namely the monolith spacecraft. If however in a given context, survivability is a critical requirement for a customer, the survivability framework here proposed, and the stochastic modeling capability developed, can demonstrate the extent to which a networked space architecture may better satisfy this requirement than a monolith spacecraft. These results should be of interest to operators whose space assets require high levels of survivability, especially in the light of emerging threats.

1. Introduction

Modeling, analyzing, and predicting failures is a central focus to many engineering disciplines dealing with system design and operations, such as civil, aerospace, and electrical engineering. Two related objectives from such a focus are: (1) to assess and rank different design options based on their propensity to and ability to cope with failures—the "analyst's" perspective; and (2) to make design choices that would (2a) prevent the occurrence of these failures or reduce the system's propensity to failures, (2b) mitigate the consequences of failures if they occur or limit their propagation throughout the system, and (2c) enable timely and effective recovery from failures—the "designer's" perspective. Given the design and development of increasingly complex and interconnected systems, it has become even more important to analyze the propensity to failures of said systems and whether they would experience catastrophic failures or graceful degradations following node or component failures for example. These failures may be triggered by endogenous or exogenous causes (e.g., attacks), and the analysis would assess, among other things, how localized failures or disruptions would propagate throughout the system. These concerns fall within the realm of survivability and resiliency analysis. A brief overview of these two concepts is provided in the next section.

In this work, we bring considerations of survivability to bear on space systems. In addition, we introduce an important tool for the modeling and analysis of stochastic processes, namely, stochastic Petri nets (SPNs), and we develop SPN models for the analysis of spacecraft survivability, building on detailed models of subsystems' multi-state failures. A framework for the quantitative analyses of system survivability is proposed and put to use, in a proof-of-concept way, for the comparative analysis of the survivability of a monolith spacecraft and space-based network. The framework here proposed, as well as the modeling and simulation capability demonstrated in this paper, should prove useful to the space industry, and government agencies who have an interest in the survivability of systems and networks.

☆This article is based on and extends previous work presented at the AIAA SPACE 2008 Conference and Exposition (paper number AIAA-2008–7707).

* Corresponding author, Tel. +1 404 385 6711; fax: +1 404 894 2760.
E-mail address: jsaleh@gatech.edu (J.H. Saleh).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.11.011

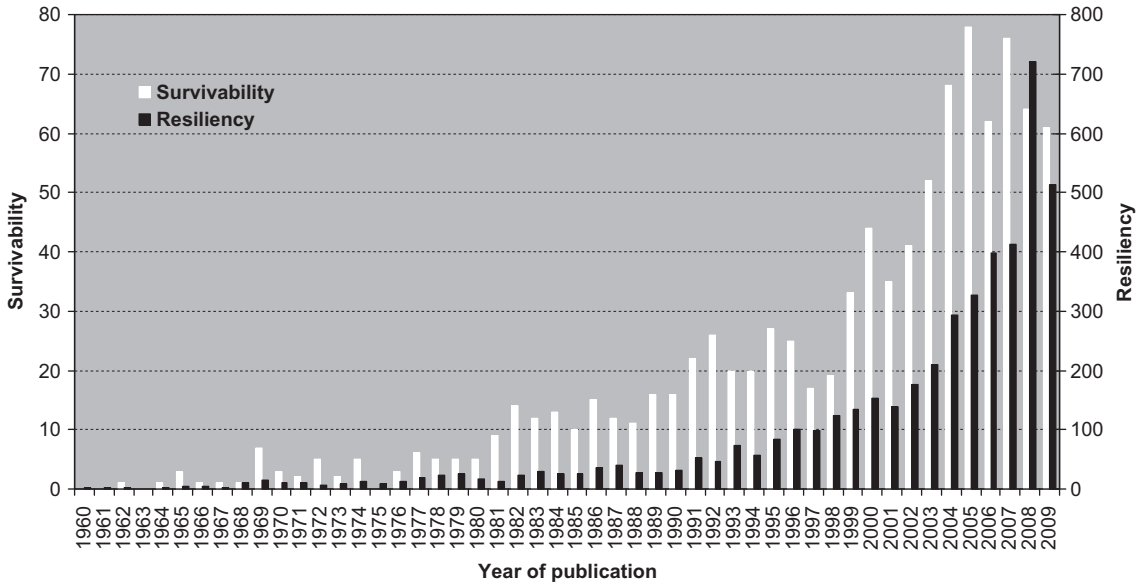

Fig. 1. Survivability and resilience/resiliency publications per year since 1960.

2. On the concepts of survivability and resiliency

In this section, we provide a brief overview of the concepts of survivability and resiliency. Although the remainder of this work focuses only on *survivability*, we briefly include *resiliency* in our discussion in this section, first to disentangle it from survivability, and second because the two concepts are sometimes used interchangeably in the literature, or one, survivability, is considered a subset or a special type of resiliency (e.g., [11]). We hope the following discussion clarifies and delineates the semantic boundary between these two concepts.

Survivability and resiliency are extensively used in the 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 Science® illustrates the growing use of these concepts in scholarly works. Fig. 1 provides a snapshot from this literature search: the first documented use of these concepts in the database[1] started in the 1960s with a handful of articles published on these subjects in the first decade, followed by a dramatic increase in the mid-1990s and that continues until today (over 60 articles were published on survivability in 2009 and more than 510 on resiliency). In addition, the interest in one particular topic, namely survivable or resilient networks, appeared in the 1980s and followed the same exponential trend.

These searches conducted on ISI Web of Science® also identify 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 are equally found and used interchangeably in publications (only the latter is used in this work).

2.1. On survivability

2.1.1. Military context

Survivability as a system attribute has always been important to the military, and its experimental and analytical assessment was probably heightened since the 1960s [1]. Survivability in a military context is applied to platforms (e.g., aircraft), people, systems (e.g., military network), and nowadays more generally to missions. Several articles show this evolution, from one of the first attempts to assess survivability of an aircraft in 1967 [1,2] to some more general definitions [3–6] 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." In addition, several publications addressed the issue of survivability of military communication networks, a growing area of interest and research since the 1990s, and for which survivability of the network is defined as the "ability to maintain communication among the nodes when it is subject to deliberate destruction" [7].

2.1.2. Engineering context

Following its initial analysis within a military context, the concept of survivability spread to other areas than the military, especially to electrical 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 community, no definition is unanimously adopted. Westmark [8] compiled 53 definitions of survivability from different publications and synthesized the following definition: survivability, according to Westmark, is "the ability of a given system with a given intended usage

[1] Used in the titles of the articles. A similar more pronounced trend is found when the search probed for these concepts in the keywords of the publications instead of the titles.