NPS-OR-07-003

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

System Availability

by

Donald P. Gaver
Patricia A. Jacobs

July 2007

Approved for public release; distribution is unlimited.

Prepared for: Director, Operational Test and Evaluation
The Pentagon, Room 3E318
Washington, D.C. 20301-1700

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA 93943-5001

VADM Daniel T. Oliver, USN (Ret.)
President

Leonard A. Ferrari
Provost

This report was prepared for and funded by the Director, Operational Test and Evaluation, The Pentagon, 3E318, Washington, D.C. 20301-1700.

This report was prepared by:

DONALD P. GAVER, JR.
Distinguished Professor Emeritus of
Operations Research

PATRICIA A. JACOBS
Professor of Operations Research

Reviewed by:

SUSAN M. SANCHEZ
Associate Chairman for Research
Department of Operations Research

Released by:

JAMES N. EAGLE
Chairman
Department of Operations Research

DAN C. BOGER
Interim Associate Provost and
Dean of Research

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** July 2007	**3. REPORT TYPE AND DATES COVERED** Technical Report	
4. TITLE AND SUBTITLE: System Availability			**5. FUNDING NUMBERS** DTAM70006
6. AUTHOR(S) Donald P. Gaver and Patricia A. Jacobs			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-OR-07-003
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Director, Operational Test and Evaluation, The Pentagon, 3E318, Washington, D.C. 20301-1700			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Availability quantifies the propensity of a system to be functionally operative upon demand. It increases if operating times between failures ("up times") are long, and decreases if, following failure or anticipatory removal, logistics delays and repair ("down times") are protracted. This chapter summarizes the general availability concept and discusses the limitation of *operational availability* suggesting that *mission availability* is often more useful and appropriate.

14. SUBJECT TERMS failure, failure mode, failure time or operating time between failures, life-testing, degradation/ageing, reliability, repair/replacement, repair/replacement time/cost, down time, availability, maintainability, safety, disposability			**15. NUMBER OF PAGES** 17
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

ABSTRACT

Availability quantifies the propensity of a system to be functionally operative upon demand. It increases if operating times between failures ("up times") are long, and decreases if, following failure or anticipatory removal, logistics delays and repair ("down times") are protracted. This chapter summarizes the general availability concept and discusses the limitation of *operational availability* suggesting that *mission availability* is often more useful and appropriate.

SYSTEM AVAILABILITY

1. OVERVIEW

All mechanical, electrical, nuclear power generation, propulsion, weapons systems, computer and data storage systems (both hard and software), communications, biological/medical, and many combinations thereof that are designed, manufactured, and tested, operated and maintained with human skills, engineering, and scientific knowledge, *are subject to failure*. This means that they become unable to perform the intended design function, or mission. *Reliability* is a measure of the propensity of component, subsystem, or system (of systems) to satisfactorily perform a required designed performance function on, say, a military or homeland security mission. This includes effectively and promptly responding to a natural disaster such as a hurricane (Katrina), tornado, or earthquake. During the period of inability to perform, the item is said to be *not available* or *unavailable*. Often this propensity is quantified as a (conditional) probability, where the conditions include stressful aspects of the operational environment and usage. Note that it is not customary to include *vulnerability* to opponent action in measures of military or security system reliability. Many, even most, failed systems are subject to failure correction or rectification, which often requires a non-negligible total *down time*, during which time interval they are completely or partially unavailable. Thus an initial informal definition of *availability* can be an estimated probability that, at the moment of demand/need for a system's performance, it will furnish that service, and not be in the process of awaiting for or being rectified/repaired/replaced. Note that field support of system availability and capability to accomplish a mission profile depends upon

sustainment resources: personnel, logistics/spare parts, tow vehicles, etc. These must also be available when needed.

It is often true that the failure propensity measure, or *hazard, or hazard rate,* of a component, subsystem, or system eventually increases with time or intensity of usage and "wear" or "age" after being fielded. Typically, a new or modified/upgraded system is tested so as to identify and remove or reduce the effect of *design defects* or *failure modes*; during the early testing period every attempt is made to induce the activation, thus exposure of, *design defects* or *failure modes*, i.e., to *stimulate* occurrences of failures and remove their causes; see [1]. Some faults inevitably remain, and can be found during routine scheduled maintenance. However, much such maintenance can be unnecessary (time-scheduled maintenance is costly in time and resources, and may well find nothing). It is currently thought to be desirable, and increasingly technically feasible, to identify and automatically track *system health* changes: failure-preceding or prognostic events (excess heat, undue vibration, wear of say tire treads, tire, engine oil condition, etc.) that can signal an incipient failure and thereby suggest needed system design or operational changes before total, possibly catastrophic, failure can occur. This procedure is known as *Condition-Based Maintenance* (*CBM*), and makes use of currently available automated embedded sensors; hence CBM+. However, the CBM+ subsystem is itself subject to malfunction and failure, so false positive and false negative diagnoses must be anticipated and made rare in order for overall gains to be made. Thus the reliability/availability of CBM+ must itself be considered as part of the total system package.

Accelerated testing procedures are often used at an early (developmental) testing stage; see [2]. During the testing phase, both Developmental and Operational, it is intended, likely, and desirable, to *find design faults and, desirably, "fix" them*, so that they will not occur/activate and cause mission-abortive events under active field conditions. It is the usual objective to test and "fix" until times between failures during testing become a stable-in-time random process, often represented by a *time-between-successive-failures distribution, with the further assumption that the times between failures are statistically independent* (*iid random variables=IIDRV*); see [2], and several computer packages, such as RELIASOFT (www.reliasoft.com).

However, initial tests of a newly designed system typically reveal "infant failures" that should be removed before any approximate stability of times-between-failures occurs. Such removal is referred to as *reliability growth*, and it has been modeled and analyzed extensively, e.g., by [3] and later [4], e.g., in the software package RELIASOFT; see also [1] for discussion of testing for growth using a sequential (run of successes) stopping rule; such testing is made more complex if the system performance is in sequential stages; failure of an early stage may mask the exposure of later stages, thus requiring longer tests so as to explore all stages for faults. After (*if*) there is evidence of failure time stochastic stability it is meaningful to speak of the *mean* (*operating*) *time between failures*; this is often specified as a reliability metric, but an estimate of the probability of mission success is usually more relevant, certainly if the item is a one-shot, or is usually-quiescent in performance: a piece of ammunition or a communication system for emergencies. Caution is required: justification for such a stable failure-time distribution must depend on actual data monitoring, and the currently appropriate

particular distributional form (model) may well depend on environmental conditions, including maintenance skill, and usage and environment; e.g., operating times between successive failures for a particular equipment (helicopter) in the Arctic can be expected to differ from those operating under tropical, sandy, desert conditions.

Upon failure, some (but not all, e.g., expendable missiles and ammunition) system components are repaired; this requires maintenance facilities and personnel, and logistics (spare parts); the system may then be again capable of performing designed-for functions. Repair or replacement is intended to restore original capability, or possibly upgrade (or, in fact, actually unintentionally and occasionally *downgrade*) system function. Preventive maintenance, based on the observed or inferred/sensed physical condition of the system, may be used to ward off catastrophic failures. As stated earlier, current attention is being focused on automated information-system-supported condition-based maintenance, or *CBM+* (alternatively, Integrated Vehicle Health Management, *IVHM*). Such subsystems continuously monitor the "health condition" of other subsystems and provide warning of imminent malfunction/failure. If successful, such a capability should allow more operative mission hours and shorter and less time-consuming and costly repairs. Success depends on the trustworthiness of the CBM+/IVHM systems available; see [5], [6], and [7].

This chapter considers that times or events between such system failures (during functional usage) are punctuated by periods of "down-time," during which the system (copy or version thereof) is (a) awaiting maintenance, which may include moving, or being moved, to a repair facility, and awaiting the arrival of parts, instrumentation, and personnel, (b) undergoing diagnosis of faults and subsequent maintenance actions, or

(c) awaiting further operational assignment (in idle standby); items may fail or degrade during such waiting/idle times, and so preliminary tests may be performed prior to mission assignment: pre-mission testing is often done, especially with aircraft and other platforms. This permits the detection of imperfect repair before the mission actually is in progress.

The (classical) System *Availability* (Ao) *parameter* is a measure of the capability of a system to *begin* to perform the designed-for function or mission *on immediate* "*random*" *demand*. Nominally, this would imply that the system is in state (c) above, but too long a sojourn of idleness, (in "cold standby") in a hostile environment can induce *startup unavailability*. *Mission availability*, measuring the capability of a system to perform its function from demand for service until mission termination is usually of far more operational significance than simple Ao. The latter is too often treated—inappropriately—as "the long-run fraction of time" (or "constant probability") that a component or system is "up" or completely mission capable at the time of demand for operation. In reality, such a constant value may not prevail; "the" value of Ao may well change with time and usage, including maintenance variation between individual copies of a system design. Often no account is taken of system age or condition, or the variable mission environment that may affect it. Further, a system's availability may be partial: e.g., a multi-engine vehicle can still function if degraded by the loss of one out of several engines. However, loss of an engine or, one of several sensors, or a communication link sometimes allows a modified or limited version of the intended mission to proceed until a replacement is furnished. Consequently, availability need not be a binary instantaneous concept.

The object of this chapter is to describe methods in use for describing, measuring, testing, and improving *Availability* and to provide cautionary comments similar to those above.

2. COMPONENT AND SYSTEM OPERATIONAL CLASSIFICATION

Engineered systems of all types are composed of numbers of components ("parts"), subsystems, and entire systems designed to perform cooperative functions. Modern warfare has been said to be conducted by "systems of systems." Such systems usually operate efficiently and effectively according to correct design, manufacture and usage. They inevitably fail or degrade with age and stress; some failure modes are mission and even life-threatening, and can occur with little warning. Hence, condition-based monitoring (CBM) and preventive maintenance (PM) are required and invoked; time spent in such makes the entity temporarily mission-unavailable, but can provide greater overall net system mission availability.

Systems, and especially subsystems and components, can be roughly categorized *as*

- *One-Shot/Disposable* (e.g., fuel, ammunition, missiles or mines, electronic components such as computer chips or screens, remote vulnerable sensors, etc.); *and*/*or*
- *Repairable* (Segmentally) - *Replaceable* (e.g., failure-prone engines and control devices, vehicle chassis, computer hardware, elements of communication networks, etc.). An injured or wounded human can sometimes be included in this category, as being part of an entire system.

In many cases, a failed repairable system becomes less susceptible to repair if too much time elapses, so the *particular item's* availability terminates, but its function is performed by a replacement or substitute; the latter can be a redesigned upgrade; see [1]. Further, the pattern of component/system usage can vary: many items, such as some sensors and alarm systems and engines and generators, are normally running or "hot" during a mission, so if failure occurs or becomes imminent, symptoms are evident. Others are normally inactive or "cold," such as an idle aircraft parked on a flight deck, or a rescue vehicle.

Many systems are made up of complex assemblies or combinations of One-Shot/Disposable *and* Repairable/Replaceable subsystems: a vehicle or platform burns fuel and may fire ammunition, both disposable, but its chassis, propulsion, and steering and sensors and communications are very often repairable/replaceable. Many vehicles operate in groups: convoys of trucks or small boats, task groups, aircraft squadrons, etc.; here the mission may involve all elements of the group, so the timely availability of such a subforce at a particular site can be spoiled if just one of the member elements fails: the entire system may become mission-incapable or unavailable if one or more of such elements fails or is damaged by opponent action (when in military or homeland protection application), or by owner/user mishandling. The tendency for such to occur is enhanced when hostilities occur, and when the sustainment/support forces and logistics are overwhelmed and themselves unavailable.

3. MODELING AVAILABILITY

System availability has been characterized probabilistically or stochastically for many years; an initial classic is [8], but aspects of repairable system availability go far

back to Erlang, Khinchine, and to Palm in the 1930s and a further few decades, well summarized in [9] as the "repairman problem" or service-system. See also [10] and [11] on survival analysis, essentially summarizing biological (e.g., animal, human "reliability"); failure-prone, but repairable, systems resemble biological epidemics: failures of subsystems can stress, or infect, other subsystems that, in turn, can cause total system collapse if not quickly isolated and mitigated.

The simplest analytical model for a failure prone, but repairable, system is the alternating renewal process (see, however, practical cautions in Section 1). Letting a sequence of up-times, $\{\boldsymbol{U}_i\}$, and a sequence of down-times, $\{\boldsymbol{D}_i\}$, be independent sequences of independent random variables with marginal distributions $F_{\boldsymbol{U}}(u;\underline{\theta})$ and $G_{\boldsymbol{D}}(v;\underline{\varphi})$, respectively, and $\underline{\theta}$ and $\underline{\varphi}$ representing parameters; then, if $A(t)$ is the availability at time t, given that the subsystem starts at the beginning of an up period, $\boldsymbol{U}_1$, say, we have the backward recurrence renewal equation

$$A(t) = P\{\boldsymbol{U}_1 > t\} + \int_0^t P\{\boldsymbol{U}_1 + \boldsymbol{D}_1 \in dx\}\, A(t-x), \tag{1}$$

which can be solved numerically or in terms of Laplace-Stieltjes transforms. Basic renewal theory asymptotics, [12], Chapter 11, shows that if $E[\boldsymbol{U}]$ and $E[\boldsymbol{D}]$ exist/are finite, then

$$\lim_{t\to\infty} A(t) = E[\boldsymbol{U}]/\left(E[\boldsymbol{U}] + E[\boldsymbol{D}]\right) = \text{Ao} \tag{2}$$

the popular (often misused) operational availability. In cases in which the system must function throughout a mission of length M a more informative measure is mission availability,

$$A_m = \mathrm{Ao}\,\frac{P\{\boldsymbol{U} > M\}}{E[\boldsymbol{U}]},$$

an asymptotic renewal theory result.

Complex systems, starting with Series/Tandem configurations, and extending to Series/Parallel/Redundant combinations can be mathematically analyzed under the initially stated independence assumptions, and with these progressively relaxed.

4. STATISTICAL INFERENCE ON AVAILABILITY

If the simple assumption of mutually independent sequences of independent identically distributed (iid) up-time r.v.s, $\{\boldsymbol{U}_i\}$ and likewise iid down times, $\{\boldsymbol{D}_i\}$ is (provisionally) acceptable then alternating renewal theory shows that the long-run *point availability* is given by $\mathrm{Ao} = E[\boldsymbol{U}]/(E[\boldsymbol{U}] + E[\boldsymbol{D}])$, provided expectations exist. A natural estimate of Ao, $\mathrm{Ao} = \bar{u}/(\bar{u} + \bar{d})$, where $\bar{u}$ and $\bar{d}$ are the sample averages of up and down realizations; assume no censoring; [13] assesses confidence intervals for Ao using jackknifing, wherein the Logit transform of Ao is recomputed, omitting pairs of observations successively. The method is applied with good success to various redundant systems and several plausible distributional forms. An alternative would be the *bootstrap* (see [14]). A sensible (semi) nonparametric approach is the nonparametric bootstrap: resample from the empirical distributions of up-and-down times, provided that preliminary examination of the data does not wildly contradict iid assumptions; see [15]. In many applied situations, data may be insufficient to validate (or invalidate) such an assumption at all conclusively. It may well be wise to adaptively smooth up and down-time means and employ these in the Ao formula. Details are available from the references.

5. CONCLUSION

Many more, and more complex, results are available from the references. For an excellent general overview see [16].

BIBLIOGRAPHY

[1] Gaver, D.P., Jacobs, P.A., Glazebrook, K.D., and Seglie, E.A., "Probability Models for Sequential-Stage System Reliability Growth via Failure Mode Removal," *International Journal of Reliability, Quality and Safety Engineering*, 10: 2003, 15-40.

[2] Meeker, W.Q. and Escobar, L.A., *Statistical Methods for Reliability Data*, John Wiley and Sons: New York, NY, 1998.

[3] Crow, L.H., "Reliability Analysis for Complex Repairable Systems," *Reliability and Biometry*, Proschan, F. and Serfling, R.J. (ed.), SIAM: Philadelphia, 1974, 379-410.

[4] Crow, L.H., "A Method for Achieving an Enhanced Mission Capability," 2002 Proc. Annual Reliability and Maintainability Symposium, IEEE: Piscataway, NJ, 2002, 153-157.

[5] Macheret, Y. and Koehn P., "Prognostics and Advanced Diagnostics for Improving Steady-State and Pulse Reliability," Proceedings 2006 IEEE Aerospace Conference, IEEE: Piscataway, NJ, 2006, 1-11.

[6] Williams, Z., "Benefits of IVHM: An Analytical Approach," Proceedings 2006 IEEE Aerospace Conference, IEEE: Piscataway, NJ, 2006, 1-8.

[7] Osborne, B., "Leveraging Remote Diagnostics Data for Predictive Maintenance," Chapter 25 in *Modern Statistical and Mathematical Methods in Reliability*, Wilson, A.G., Limnios, N., Keller-McNulty, S., and Armijo, Y. (ed.), World Scientific Publishing Co.: Singapore, 2005, 353-373.

[8] Barlow, R.E. and Proschan, F., *Mathematical Theory of Reliability*, Wiley: New York, NY, 1967.

[9] Feller, W., *An Introduction to Probability Theory and its Applications*, Vol. 1, 3rd Ed., Wiley: New York, NY, 1968.

[10] Cox, D.R., *Renewal Theory*, Methuen & Co: London, 1970.

[11] Cox, D.R. and Oakes, D., *Analysis of Survival Data*, Chapman and Hall: London, 1984.

[12] Feller, W., *An Introduction to Probability Theory and its Applications*, Vol. 2, Wiley: New York, NY, 1966.

[13] Gaver, D.P. and Chu, B.B., "Jackknife Estimates of Component and System Availability," *Technometrics*, 21: 1979, 443-450.

[14] Efron, B. and Tibshirani, R.J., *An Introduction to the Bootstrap*, Chapman and Hall: New York, NY, 1993.

[15] Gaver, D.P. and Jacobs, P.A., "System Availability: Time Dependence and Statistical Inference by (Semi) Non-Parametric Methods," *Applied Stochastic Models and Data Analysis*, 5: 1989, 357-375.

[16] Davis, T.P., "Science, Engineering, and Statistics," *Applied Stochastic Models in Business and Industry*, 22: 2006, 401-430.

INITIAL DISTRIBUTION LIST

1. Research Office (Code 09) 1
   Naval Postgraduate School
   Monterey, CA 93943-5000

2. Dudley Knox Library (Code 013) 2
   Naval Postgraduate School
   Monterey, CA 93943-5002

3. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

4. Richard Mastowski (Technical Editor) 2
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, CA 93943-5219

5. Distinguished Professor Donald P. Gaver 4
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93943-5219

6. Professor Patricia A. Jacobs 4
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93943-5219

7. Dr. Ernest Seglie ..... electronic copy

8. Dr. Arthur Fries ..... electronic copy

9. Dr. John Lehoczky ..... electronic copy

10. Dr. Kevin Glazebrook ..... electronic copy

11. Professor Min Xie ..... electronic copy

12. Professor Lyn Thomas ..... electronic copy

13. Professor Ramalhoto ..... electronic copy

14. Dr. Chiu ..... electronic copy

15. Dr. Alyson Gabbard Wilson ..... electronic copy

16. Professor Tim Bedford.....electronic copy

17. Dr. J. Norstrom .....electronic copy

18. Dr. Paul Ellner .....electronic copy

19. Dr. G. Latouche.....electronic copy

20. Dr. G. Fayolle .....electronic copy

21. Professor Kolowrocki .....electronic copy

22. Professor M. Nikouline.....electronic copy

23. Dr. F. Samaniego .....electronic copy