General Disclaimer

One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.

- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.

- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.

- This document is paginated as submitted by the original source.

- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

Produced by the NASA Center for Aerospace Information (CASI)

J. F. Meyer
D. G. Puchtgott
A. Movaghar

January 1982

Prepared for National Aeronautics and Space Administration
Langley Research Center
Hampton, Virginia 23365

G. E. Migneault—NASA Technical Officer
NASA Grant NSG 1306

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
SYSTEMS ENGINEERING LABORATORY
THE UNIVERSITY OF MICHIGAN, ANN ARBOR 48109
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1. Specification Bibliography</td>
<td>4</td>
</tr>
<tr>
<td>2. Design Bibliography</td>
<td>15</td>
</tr>
<tr>
<td>3. Verification Bibliography</td>
<td>23</td>
</tr>
<tr>
<td>4. Testing Bibliography</td>
<td>27</td>
</tr>
<tr>
<td>5. Evaluation Bibliography</td>
<td>28</td>
</tr>
</tbody>
</table>
0. Introduction

There is a body of literature describing formal methods which have been or are being developed to support the design and development of various "real-time" systems. We are referring here, more specifically, to systems which operate in real-time computation/control/communication environments where timeliness is a principal requirement. (Excluded, therefore, are so-called "on-line" environments such as airline reservations and inventory control where timing demands are less severe.) In addition to timeliness, these systems must typically satisfy other needs that are characteristic of avionic and control applications, e.g., needs for fault-tolerance, degradable performance, distributed architectures, and concurrent (parallel) execution of tasks. Accordingly, many design and validation problems precipitated by these needs are common, in varying degrees and forms, to a variety of real-time systems. Along with avionic systems, these include other vehicle control systems (for spacecraft, trains, etc.), telephone switching systems, power distribution systems, computer/communication networks, manufacturing process control systems, computer operating systems, and parallel programs.

With respect to these various types of real-time systems, the development of formal design and validation methods (with the exception of formal evaluation methods) has been pursued, most actively, in the context of computer operating systems and parallel programs. Although such systems are considerably less complex than a fully integrated avionic system, we believe this activity is representative of approaches that must be taken in the avionic system context. In particular, we are referring here to work on formal specifications, design languages, verification, and testing.

This report contains the results of a literature survey designed to classify current literature on formal methods that might be meaningfully exploited in
the specification, design, and validation of avionic systems (where validation includes verification, testing and evaluation). The specific literature searched includes journal papers, conference papers, and technical reports published during the last five years (beginning in 1977). The articles are classified according to five topic areas: specification, design, verification, testing and evaluation. Because the survey was completed in September 1981, no citations appearing after that date are included in the resulting bibliography.

Two search modes were employed: a manual search of the major journals and conference proceedings dealing with these areas, and a computer search using automatic information retrieval services that exist at The University of Michigan. Among the sources consulted for the manual search were *IEEE Transactions on Computers*, *IEEE Transactions on Software Engineering*, *IEEE Transactions on Reliability*, *Journal of the ACM*, *Communications of the ACM*, *Proceedings of the International Symposium on Fault Tolerant Computing*, and the bibliographies associated with the relevant articles in those sources. Where possible, the bibliographies of the articles referred to by the first set of articles were consulted, and the process was iterated. The automatic search was performed using the facilities of Dialog Informations Services, Inc. of Palo Alto, CA. The specific data bases accessed were INSPEC [1977 to present] (The Institution of Electrical Engineers) and COMPENDEX [1971 to present] (Engineering Index, Inc.). Keywords used were

<table>
<thead>
<tr>
<th>Specification</th>
<th>Verification</th>
<th>Testing</th>
<th>Design</th>
<th>Implementation</th>
<th>Stochastic</th>
<th>Formal</th>
<th>Mathematical</th>
<th>Theoretical</th>
<th>Petri Net</th>
<th>Abstract Data Type</th>
<th>Initial Algebra</th>
<th>Data Abstraction</th>
</tr>
</thead>
</table>

Citations having at least one keyword from each of column 1 and column 2 were
flagged. In some cases, many citations were found for one of the above combinations; additional words were then used to narrow the number of hits. These words included "top down", "bottom up", "hierarchical", and "parallel."

The report is divided into five sections, corresponding to the five topic areas: specification, design, verification, testing, and evaluation. Bibliographic entries are listed according to the topic(s) they apply to. Hence, if an article relates (appreciably) to more than one topic, its reference is listed in each applicable section. Also, entries are listed first by year of publication, and then within the year, alphabetically by the primary author's last name.
1. Specification Bibliography


2. Design Bibliography


3. Verification Bibliography


4. Testing Bibliography


5. Evaluation Bibliography


