AIAA
G-118-2006

Guide

Managing the Use of Commercial Off the Shelf (COTS) Software Components for Mission-Critical Systems

AIAA
G-118-2006

Guide

Managing the Use of Commercial Off the Shelf (COTS) Software Components for Mission-Critical Systems

Sponsored by

American Institute of Aeronautics and Astronautics

Approved

13 October 2006

Abstract

The purpose of this Guide is to assist development and maintenance projects (teams and individuals) that have to address the use of, or consideration of, COTS products within large, complex systems, including but not limited to mission critical systems. This assistance is provided by capturing a set of information about COTS products (benefits, risks, recommended practices, lifecycle activity impacts) and mission critical systems (variety of MCS, special needs for MCS, differences between MCS and other types of systems) and then providing some linkage between these topics so that various types of stakeholders can find useful information. The document should be of value to both management and technical individuals/teams. It should also be of value to teams that are dealing with non-MCS, in that the scope is not limited to only MCS.

Managing the use of commercial off the shelf (COTS) software components for mission-critical systems : AIAA G-118-2006 guide.

p. cm.

Includes bibliographical references.

ISBN 1-56347-915-X (print) -- ISBN 1-56347-916-8 (electronic)

1. Aeronautics--Computer programs. 2. Astronautics--Computer programs. 3. Astronautics--United States--Equipment and supplies. 4. Software engineering. 5. Commercial products. I. American Institute of Aeronautics and Astronautics.

TL563.M36 2006

629.10285'5--dc22

2006039308

Published by
American Institute of Aeronautics and Astronautics
1801 Alexander Bell Drive, Reston, VA 20191

Printed in the United States of America

Contents

Figures

Tables

Foreword

Commercial off-the-shelf (COTS) products are being considered for inclusion in ever more complex and critical systems. There are clear advantages to considering the use of COTS in such complex or critical systems but given the rigorous needs of such critical systems or subsystems, there have begun to emerge concerns about the suitability of COTS for such applications. This guide identifies some of the characteristics of mission critical systems (MCS) that make the selection process of COTS products (hardware, software, subsystems, etc., but especially software) an emerging success factor in total system acceptance.

Mission critical system characteristics such as reliability, safety, availability, maintainability and certification tend to influence whether or not COTS should be considered for a given application. Once the suitability of COTS has been determined it may be possible to place additional requirements on the product and/or the product's vendor for such mission critical applications. Further, it is possible that certain system requirements and expectations may need to be modified because of the inclusion of COTS products into that system. As COTS products continue to be considered as candidates for inclusion within MCS, there are likely to be additional concerns and factors to emerge that will influence how both buyers and vendors decide if and/or when to use COTS products. The benefits and risks of using COTS in MCS are detailed in this guide. Risk mitigation approaches applicable to the selection and usage of COTS software components in MCS are discussed as they apply to the software product lifecycle.

This guide was initially focused on the use of COTS software products in MCS. As it was developed, it quickly became clear that some/much of what was being captured applied to COTS products other than just software. It also became evident to the committee that much of what was being captured applied to non-MCS. This guide will be most useful and applicable to large, complex systems that are considering or actually using COTS software products. The user is also likely to find this guide of value in COTS hardware projects as well as to systems that range from spacecraft and aerospace applications to human resource or financial applications. In addition, this guide can apply to test hardware and software.

This Guide was produced under the auspices of the Software Systems Technical Committee (SSTC) of the American Institute of Aeronautics and Astronautics (AIAA). It was initially conceived by Ronald J. Kohl, of R. J. Kohl & Associates who provided substantial content. The document was then transferred to the AIAA Software Systems Committee on Standards (CoS) for further review and formal approval as an AIAA standards document.

At the time of approval, the members of the AIAA **Software Systems CoS** were:

Ronald J. Kohl, Chair	R.J. Kohl & Associates
Rick Kwan	Aerospace Computing, Inc.
Joe Marshall	BAE Systems
A. Terry Morris	NASA Langley Research Center
Shawn Rahmani	The Boeing Company
Nancy Sodano	The Charles Stark Draper Laboratory, Inc.

The above consensus body approved this document in October 2006.

The AIAA Standards Executive Council (Amr ElSawy, Chairman) accepted the document for publication in October 2006.

The AIAA Standards Procedures dictates that all approved Standards, Recommended Practices, and Guides are advisory only. Their use by anyone engaged in industry or trade is entirely voluntary. There is no agreement to adhere to any AIAA standards publication and no commitment to conform to or be guided by standards reports. In formulating, revising, and approving standards publications, the

committees on standards will not consider patents that may apply to the subject matter. Prospective users of the publications are responsible for protecting themselves against liability for infringement of patents or copyright or both.

Introduction

It should be noted that although the intent of this Guide is to focus on COTS software products and their use in large, complex software-based systems, it does contain guidance that can apply to certain aspects of COTS hardware utilization. Some of this guidance can also be applied to non-developed items (NDI) types of software other than COTS, such as open source software, reusable component software and even shareware/freeware software. These other applications are not highlighted or discussed specifically herein but are mentioned to encourage users to think broadly and across many problematic areas to determine if there is additional value contained in this document that may be applicable.

It should be noted that this guide may be used for managing the risks associated with the use of COTS products in large, complex systems utilizing the mapping of the 'Recommended Practices' to the 'Risk areas'. Sections 8 and 9 discuss how these various practices and processes can be applied across the software systems lifecycle, therefore helping to establish or improve the set of software and systems development processes.

1 Scope

The purpose of this Guide is to assist development and maintenance projects (teams and individuals) that have to address the use of, or consideration of, COTS products within large, complex systems, including but not limited to mission critical systems. This assistance is provided by capturing a set of information about COTS products (benefits, risks, recommended practices, lifecycle activity impacts) and mission critical systems (variety of MCS, special needs for MCS, differences between MCS and other types of systems) and then providing some linkage between these topics so that various types of stakeholders can find useful information. The document should be of value to both management and technical individuals/teams. It should also be of value to teams that are dealing with non-MCS, in that the scope is not limited to only MCS.

2 Applicable Documents

The following documents contain provisions, which, through reference in this text, constitute provisions of this guide. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this guide are encouraged to investigate the possibility of applying the most recent editions of the applicable documents indicated below. For undated references, the latest edition of the applicable document referred to applies.

IEEE/EIA 12207	*Industry Implementation of ISO/IEC 12207:1995 — Standard for Information Technology — Software Life Cycle Processes*
ISO 9126	*Software engineering -- Product quality -- Part 1: Quality model*
NASA-STD-8719.13B	*Software Safety Standard*
NASA-GB-8719.13	*NASA Software Safety Guidebook*
RTCA DO-178B	*Software Considerations in Airborne Systems and Equipment Certification*

3 Vocabulary

3.1 Acronyms and Abbreviated Terms

AIAA	American Institute of Aeronautics and Astronautics
CM	Configuration Management
CBS	COTS-based System or Systems
CMM	Capability Maturity Model
COTS	Commercial Off-The-Shelf
DOD	Department of Defense
FAA	Federal Aviation Administration
MCS	Mission Critical System or Systems
MOTS	Modified Off The Shelf
NAD	No Additional Detail provided
NASA	National Aeronautics and Space Administration
NDI	Non Development Items