OETCS/WP7/O7.1.3_O7.1.7 – 00/01

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

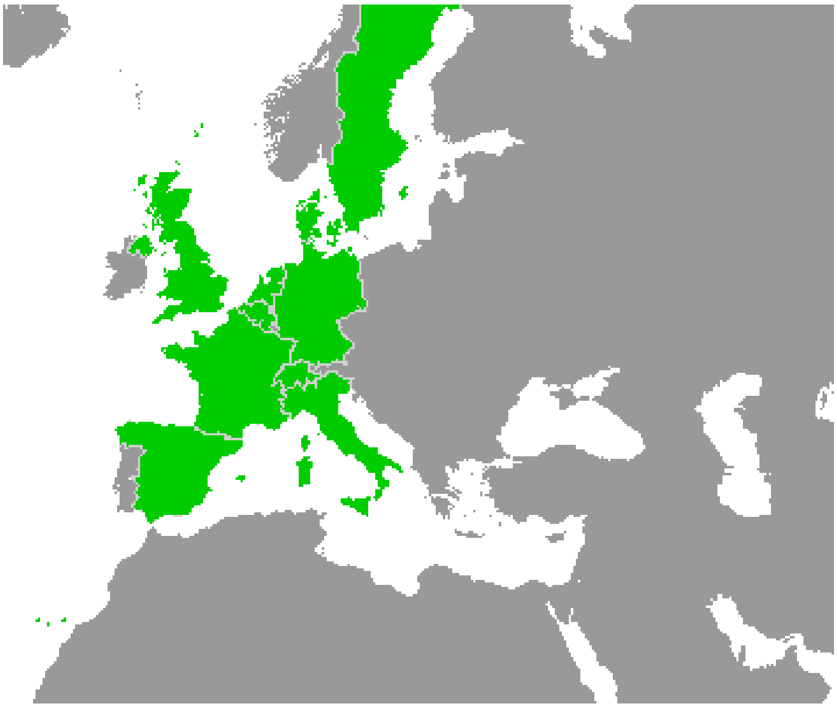
Work-Package 7: “Primary tool chain”

Evaluation of the models and tools against the WP2 requirements

List of criteria on means, models and tools and results on the benchmark

Marielle Petit-Doche

April 2013



This work is licensed under the European Union Public Licence (EUPL v.1.1) a Creative Commons Attribution-ShareAlike 3.0 Unported License.

This page is intentionally left blank

Work-Package 7: “Primary tool chain”

OETCS/WP7/O7.1.3_O7.1.7 – 00/01
April 2013

Evaluation of the models and tools against the WP2 requirements

List of criteria on means, models and tools and results on the benchmark

Marielle Petit-Doche

Systerel

Definition

This work is licensed under the European Union Public Licence (EUPL v.1.1) a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Prepared for ITEA2 openETCS consortium
Europa

Abstract: This document gives elements to evaluate the means of modeling and the associated tools according WP2 requirements. Evaluation on the models and tools of benchmark is also described.

Disclaimer: This work is licensed under the European Union Public Licence (EUPL v.1.1) and a Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

http://creativecommons.org/licenses/by-sa/3.0/
http://joinup.ec.europa.eu/software/page/eupl/licence-eupl

Table of Contents

Figures and Tables

Figures

Tables

Document information	
Work Package Deliverable ID or doc. ref.	WP7 O7.3.1_O7.1.7
Document title Document version Document authors (org.)	Evaluation of the models and toolsagainst the WP2 requirements 00.01 Marielle Petit-Doche (Systerel)

Review information	
Last version reviewed	00.00.00
Main reviewers	

Approbation			
	Name	Role	Date
Written by	Marielle Petit-Doche	WP7-T7.1 Sub-Task Leader	
Approved by	Michael Jastram	WP7 leader	

Document evolution			
Version	Date	Author(s)	Justification
00.00.01	19/04/2013	M. Petit-Doche	Document creation by merging O7.1.3 and O7.1.7

1 Introduction

The aim of this document is to report the results of the evaluation of the means of description to model the requirements of SUBSET-026 concerning the on-board unit and their assocaited tools.

This evaluation task is part on work package WP7, task 1 "Primary tool Chain analyses and recommendations". According to the results of WP2, especially the OpenETCS process and the requirements on language, the aim of this task is to determine the best candidates to produce models of the on-board units, following the OpenETCS process

This process is described in détail in D2.3 " Description of the openETCS process" and is summed up in the figure 2.

Yellow elements are inputs, blue elements are part of the design process, red elements are verification and validation activities, green elements are safety activities. Each line (between dash or full blue lines) is a phase of the process, with a name on the right.

The second section of this document provides a template to describe the means and tools and a list of criteria according WP2 requirements on language, models and tools. The objectives of this description and criteria are to allow to determine the best means of description and associated tool for a given activities.

The third section resumes the results of the evaluation at the end of the benchmark activities.

In Appendix, a section is dedicated to each models produced during the benchmark activities :

- CORE
- GOPRR
- ERTMSFormalSpecs
- SysML with Papyrus
- SysML with Entreprise Architect
- SCADE
- EventB with Rodin
- Classical B with Atelier B
- Petri Nets
- System C
- GNATprove

For each approach and tool, the initial author of the evaluation is the partner in charge of the modelling. Two assessors, for each approaches, are in charge of the review of the evaluation and can correct it or add comments.

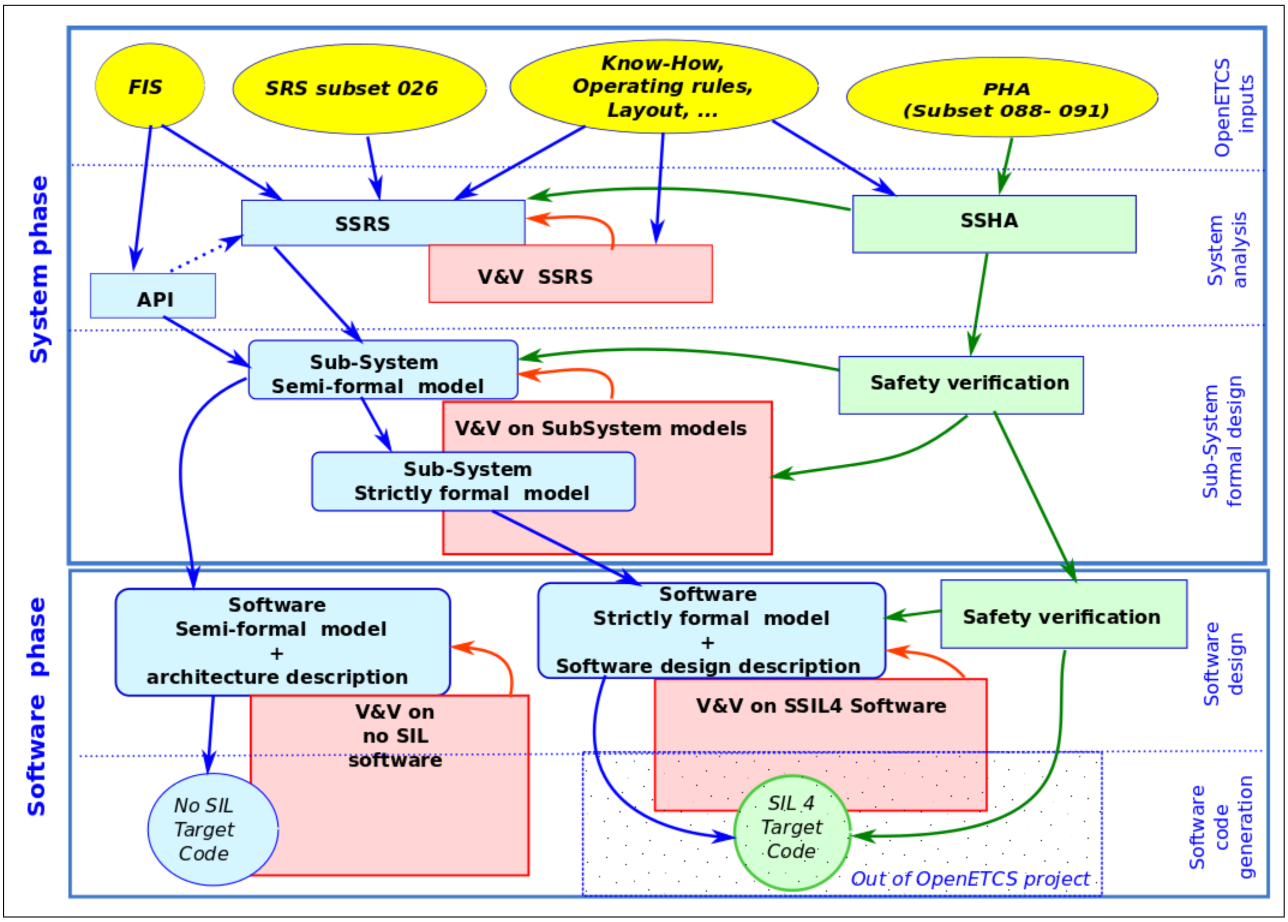


Figure 1. Main OpenETCS process

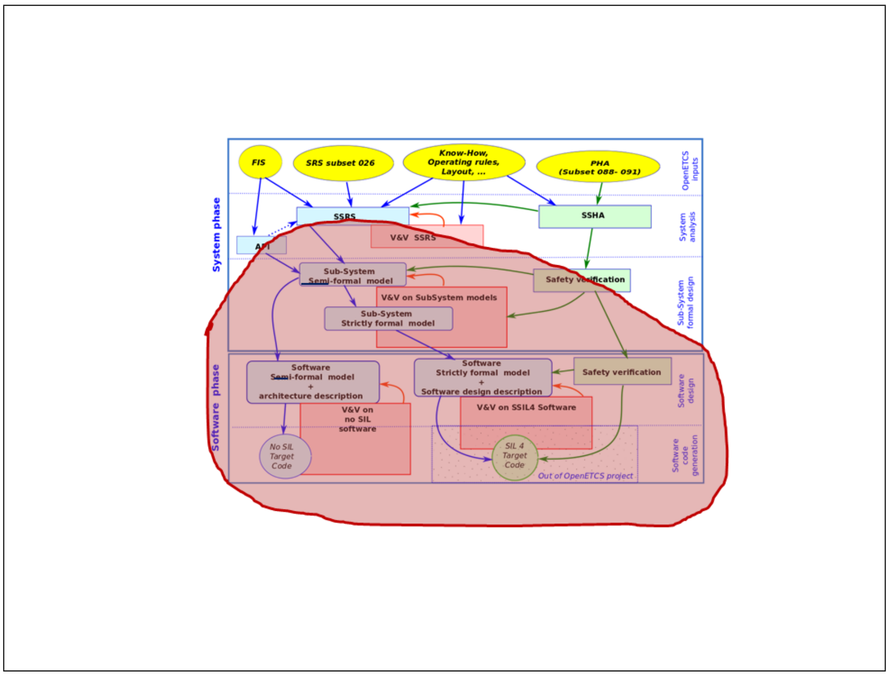


Figure 2. SCADE coverage of the OpenETCS process

Tool platform are not covered by this document but in an other output of WP7 : O7.1.9 "Evaluation of each tool platform against WP2 requirements, independent of target tools". Besides, Task 7.1 is focussing on design activities : despite that some means can provide verification artefacts for example, tools and means for validation, verification, test generation,... are in the scope of task 2 and will be analysed later.

2 Templates

Author Author of the approaches description %%Uwe Steinke - Siemens AG%%

Assessor 1 First assessor of the approaches %%Name - Company%%

Assessor 2 Second assessor of the approaches %%Name - Company%%

In the sequel, main text is under the responsibilities of the author.

> *Author.* *Author can add comments using this format*

> *Assessor 1.* *First assessor can add comments using this format*

> *Assessor 2.* *Second assessor can add comments using this format*

When a note is required, please follow this list :

0 not recommended, not adapted, rejected

1 weakly recommended, adapted after major improvements, weakly rejected

2 recommended, adapted (with light improvements if necessary) weakly accepted

3 highly recommended, well adapted,strongly accepted

***** difficult to evaluate with a note (please add a comment under the table)

All the notes can be commented under each table.

2.1 Presentation

This section gives a quick presentation of the approach and the tool.

Name Name of the approach and the tool

Web site if available, how to find information

Licence Kind of licence

Abstract

Short abstract on the approach and tool (10 lines max)

Publications

Short list of publications on the approach (5 max)

2.2 Main usage of the approach

This section discusses the main usage of the approach.

According to the figure 2, for which phases do you recommend the approach (give a note from 0 to 3) :

	Author	Assessor 1	Assessor 2	Total
System Analysis	1			
Sub-system formal design	3			
Software design	3			
Software code generation	3			

> *Author. SCADE can be used for analyzing tasks on system level, especially to clarify complex system behaviour and functions by practical modelling, execution, simulation and test. For a higher abstraction level, this should be enhanced with system modelling languages as SysML.*

According to the figure 2, for which type of activities do you recommend the approach (give a note from 0 to 3) :

	Author	Assessor 1	Assessor 2	Total
Documentation	3			
Modeling	3			
Design	3			
Code generation	3			
Verification	3			
Validation	3			
Safety analyses	0			

Known usages

Have you some examples of usage of this approach to compare with the OpenETCS objectives ?

2.3 Language

This section discusses the main element of the language.

According WP2 requirements, give a note for the characteristics of the language (from 0 to 3) :

	Author	Assessor 1	Assessor 2	Total
Informal language	0			
Semi-formal language	0			
Formal language	3			
Structured language	3			
Modular language	3			
Extensible language (D.2.6-01-28)	2			
Textual language	3			
Mathematical symbols or code	3			
Graphical language	3			
Declarative and simple formalization of properties (D.2.6-X-27)	2			
Scalability : capability to design large model	3			
Easily translatable to other languages (D.2.6-X-28)	3			
Executable	3			
Simulation, animation	3			
Easily understandable (D.2.6-X-26)	3			
Expertise level needed (0 High level, 3 few level)	3			
Standardization	3			

> *Author. SCADE is a strictly textual and graphical formal language. It allows to be extended with user-defined operators. Especially the graphical representation is easy to learn and understand; nevertheless the rich tool suite covering most aspects of a EN50128 compliant process causes an appropriate learning effort by amount.*

Documentation

Describe how the language is documented, the existing guidelines, coding rules, standardization...

Language usage

Describe the possible restriction on the language

2.4 System Analysis

This section discusses the usage of the approach for system analysis. It can be skipped depending the results of 2.8.

Acoording WP2 requirements, how the approach can be involved for the sub-system requirement specification ?

	Author	Assessor 1	Assessor 2	Total
Independent System functions definition (D.2.6-X-10.1.1)	3			
System architecture design (D.2.6-X-10.1.2)	1			
System data flow identification (D.2.6-X-10.1.3)	3			
Sub-system focus (D.2.6-X-10.1.4)	2			
System interfaces definition (D.2.6-X-10.1.5)	2			
System requirement allocation (D.2.6-X-10.2)	3			
Traceability with SRS (D.2.6-X-10.3)	3			
Traceability with Safety activities (D.2.6-X-11)	3			

Author. Although SCADE is not made for system analysis, it can be used for the following aspects on system level: Modelling of (separate) system functions, data flows, state machines and interfaces. It provides an excellent tracebility support between many different kinds of documents and other tools.

2.5 Sub-System formal design

This section discusses the usage of the approach for sub-system formal design. It can be skipped depending the results of 2.8.

2.5.1 Semi-formal model

Author. SCADE models are formal. Since the following table addresses many aspects that SCADE covers in a formal way it is filled anyway. But keep in mind: it's formal - instead of semi-formal.

Concerning formal model, how the WP2 requirements are covered ?

	Author	*Assessor 1*	*Assessor 2*	*Total*
Consistency to SSRS (D.2.6-X-12.2)	*2*			
Coverage of SSRS (D.2.6-X-12.2.1)	*3*			
Traceability to SSRS (D.2.6-X-12.3)	*3*			
Simulation or animation (D.2.6-X-13 partial)	*3*			
Execution (D.2.6-X-13 partial)	*3*			
Extensible to strictly formal model (D.2.6-X-14.3)	*3*			
Easy to refine towards strictly formal model (D.2.6-X-14.4)	*3*			
Extensible and modular design (D.2.6-X-15)	*3*			
Extensible to software design (???)	*3*			
Safety properties formalisation (D.2.6-01-20)	*2*			
Safety properties validation (D.2.6-X-22 partial)	*2*			
Logical properties assertion (D.2.6-X-32)	*2*			
Check of assertions (D.2.6-X-32.1)	*2*			

Author. SCADE is a modelling language for functions. Therefore, only the functional aspects of properties are addressed.

Does the language allow to formalize (D.2.6-X-29):

	Author	*Assessor 1*	*Assessor 2*	*Total*
State machines	*3*			
Time-outs	*3*			
Truth tables	*3*			
Arithmetic	*3*			
Braking curves	*3*			
Logical statements	*3*			
Message and fields	*3*			

Additional comments on semi-formal model

Do you think your semi-formal model is sufficient to cover a safe design of the on-board unit until code generation ? All comments on links to other models, validation and verification activities are welcomed.

2.5.2 Strictly formal model

Concerning strictly formal model, how the WP2 requirements are covered ?

	Author	*Assessor 1*	*Assessor 2*	*Total*
Consistency to SFM (D.2.6-X-14.2)	*3*			
Coverage of SSRS (D.2.6-X-14.2)	*3*			
Traceability to SSRS (D.2.6-X-14.3)	*3*			
Extensible to software design (D.2.6-X-16)	*3*			
Safety properties formalisation (D.2.6-01-20)	*2*			
Safety properties validation (D.2.6-X-22 partial)	*2*			
Logical properties assertion (D.2.6-X-32)	*2*			
Check of assertions (D.2.6-X-32.2)	*2*			

Does the language allow to formalize (D.2.6-X-30):

	Author	*Assessor 1*	*Assessor 2*	*Total*
State machines	*3*			
Time-outs	*3*			
Truth tables	*3*			
Arithmetic	*3*			
Braking curves	*3*			
Logical statements	*3*			
Message and fields	*3*			

Additional comments on semi-formal model

Do you think your strictly formal model can be directly defined from the SSRS ? All comments on links to other models, validation and verification activities are welcomed.

2.6 Software design

This section discusses the usage of the approach for software design. It can be skipped depending the results of 2.8.

2.6.1 Functional design

How the approach allows to produce a functional software model of the on-board unit ?

	Author	Assessor 1	Assessor 2	Total
Derivation from system semi-formal model	3			
Software architecture description	3			
Software constraints	3			
Traceability	3			
Executable	3			

2.6.2 SSIL4 design

How the approach allows to produce in safety a software model ?

	Author	Assessor 1	Assessor 2	Total
Derivation from system semi-formal or strictly formal model	3			
Software architecture description	3			
Software constraints	3			
Traceability	3			
Executable	3			
Conformance to EN50128 § 7.2	3			
Conformance to EN50128 § 7.3	3			
Conformance to EN50128 § 7.4	3			

Which criteria for software architecture are covered by the methodology (see EN50128 table A.3) :

	Author	Assessor 1	Assessor 2	Total
Defensive programming	3			
Fault detection & diagnostic	0			
Error detecting code	0			
Failure assertion programming	1			
Diverse programming	0			
Memorising executed cases	0			
Software error effect analysis	0			
Fully defined interface	3			
Modelling	3			
Structured methodology	3			

2.7 Software code generation

This section discusses the usage of the approach for software code generation. It can be skipped depending the results of 2.8.

Which criteria for software design and implementation are covered by the methodology (see EN50128 table A.4) :

	Author	Assessor 1	Assessor 2	Total
Formal methods	3			
Modeling	3			
Modular approach (mandatory)	3			
Components	3			
Design and coding standards (mandatory)	3			
Strongly typed programming language	3			

2.8 Main usage of the tool

This section discusses the main usage of the tool.

Which task are covered by the tool ?

	Author	*Assessor 1*	*Assessor 2*	*Total*
Modelling support	*3*			
Automatic translation	*3*			
Code Generation	*3*			
Model verification	*3*			
Test generation	*2*			
Simulation, execution, debugging	*3*			
Formal proof	*3*			

Modelling support

Does the tool provide a textual or a graphical editor ?

Automatic translation and code generation

Which translation or code generation is supported by the tool ?

Model verification

Which verification on models are provided by the tool?

Test generation

Does the tool allow to generate tests ? For which purpose ?

Simulation, execution, debugging

Does the tool allow to simulate or to debbug step by step a model or a code ?

Formal proof

Does the tool allow formal proof ? How ?

2.9 Use of the tool

According WP2 requirements, give a note for characteristics of the use of the tool (from 0 to 3) :

	Author	*Assessor 1*	*Assessor 2*	*Total*
Open Source (D2.6-01-029)	*0*			
Portability to operating systems (D2.6-01-030)	*3*			
Cooperation of tools (D2.6-01-031)	*3*			
Robustness (D2.6-01-034)	*3*			
Modularity (D2.6-01-034.01)	*3*			
Documentation management (D.2.6-01-034.02)	*3*			
Distributed software development (D.2.6-01-034.03)	*2*			
Issue tracking (D.2.6-01-034.04)	*0*			
Differences between models (D.2.6-01-034.05)	*3*			
Version management (D.2.6-01-034.06)	*3*			
Concurrent version management (D.2.6-01-034.07)	*3*			
Model-based version control (D.2.6-01-034.08)	*3*			
Role traceability (D.2.6-01-034.09)	*0*			
Safety version traceability (D.2.6-01-034.10)	*0*			
Model traceability (D.2.6-01-035)	*3*			
Tool chain integration	*3*			
Scalability	*3*			

2.10 Certifiability

This section discusses how the tool can be classified according EN50128 requirements (D.2.6-X-49).

	Author	*Assessor 1*	*Assessor 2*	*Total*
Tool manual (D.2.6-01-42.02)	*3*			
Proof of correctness (D.2.6-01-42.03)	*3*			
Existing industrial usage	*3*			
Model verification	*3*			
Test generation	*2*			
Simulation, execution, debugging	*3*			
Formal proof	*3*			

Other elements for tool certification

2.11 Other comments

Please to give free comments on the approach.

3 Conclusion

%%To Be Defined%%

- *CORE*
- *GOPRR*
- *ERTMSFormalSpecs*
- *SysML with Papyrus*
- *SysML with Entreprise Architect*
- *SCADE*
- *EventB*
- *Classical B*
- *Petri Nets*
- *System C*
- *GNATprove*

CC BY-SA

Appendix: References

[1] *US Army Corps of Engineers, Engineer Research and Development Center.* Guide for Preparing Technical Information Reports of the Engineer Research and Development Center*, January 2006.*

[2] *Walter Schmidt.* Using Common PostScript Fonts With LaTeX. PSNFSS Version 9.2*, September 2004.* `http://ctan.tug.org/tex-archive/macros/latex/required/psnfss`.

[3] *Hideo Umeki.* The geometry Package*, December 2008.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/geometry`.

[4] *Piet van Oostrum.* Page Layout in LaTeX*, March 2004.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/fancyhdr`.

[5] *D. P. Carlisle.* Packages in the 'Graphics' Bundle*, November 2005.* `http://ctan.tug.org/tex-archive/macros/latex/required/graphics`.

[6] *UK TEX Users Group. UK list of TEX frequently asked questions.* `http://www.tex.ac.uk/cgi-bin/texfaq2html`*, 2006.*

[7] *Leslie Lamport.* LaTeX: a Document Preparation System. *Addison-Wesley Publishing Company, Reading, Ma., 2 edition, 1994. Illustrations by Duane Bibby.*

[8] *Department of Defense, Washington, DC.* Distribution Statements on Technical Documents. DoD Directive 5230.24*, 1987.*

[9] *Axel Sommerfeldt.* Typesetting Captions with the caption Package*, February 2007.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/caption`.

[10] *Patrick W. Daly.* Natural Sciences Citations and References (Author-Year and Numerical Schemes)*, February 2009.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/natbib`.

[11] *Michael Downes and Barbara Beeton.* The amsart, amsproc, and amsbook document classes. *American Mathematical Society, August 2004.* `http://www.ctan.org/tex-archive/macros/latex/required/amslatex/classes`.

[12] *David Carlisle.* The longtable Package*, February 2004.* `http://www.ctan.org/tex-archive/macros/latex/required/tools`.

[13] *Martin Schröder.* The ragged2e Package*, March 2003.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/ms`.

[14] *Leslie Lamport, Frank Mittelbach, and Johannes Braams.* Standard Document Classes for LaTeX version 2e*, 1997.* `http://ctan.tug.org/tex-archive/macros/latex/base`.

[15] *David Carlisle.* The dcolumn Package*, May 2001.* `http://ctan.tug.org/tex-archive/macros/required/tools`.

[16] *American Mathematical Society.* User's Guide for the amsmath Package (Version 2.0)*, February 2002.* `http://ctan.tug.org/tex-archive/macros/`

latex/required/amslatex/math/amsldoc.pdf.

[17] *Boris Veytsman.* LaTeX Support for Microsoft Georgia and ITC Franklin Gothic In Text and Math, *July 2009.* *http://ctan.tug.org/tex-archive/fonts/mathgifg/*.

Appendix: References

[1] *US Army Corps of Engineers, Engineer Research and Development Center.* Guide for Preparing Technical Information Reports of the Engineer Research and Development Center*, January 2006.*

[2] *Walter Schmidt.* Using Common PostScript Fonts With LaTeX. PSNFSS Version 9.2*, September 2004.* `http://ctan.tug.org/tex-archive/macros/latex/required/psnfss`*.*

[3] *Hideo Umeki.* The geometry Package*, December 2008.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/geometry`*.*

[4] *Piet van Oostrum.* Page Layout in LaTeX*, March 2004.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/fancyhdr`*.*

[5] *D. P. Carlisle.* Packages in the 'Graphics' Bundle*, November 2005.* `http://ctan.tug.org/tex-archive/macros/latex/required/graphics`*.*

[6] *UK TeX Users Group. UK list of TeX frequently asked questions.* `http://www.tex.ac.uk/cgi-bin/texfaq2html`*, 2006.*

[7] *Leslie Lamport.* LaTeX: a Document Preparation System. *Addison-Wesley Publishing Company, Reading, Ma., 2 edition, 1994. Illustrations by Duane Bibby.*

[8] *Department of Defense, Washington, DC.* Distribution Statements on Technical Documents. DoD Directive 5230.24*, 1987.*

[9] *Axel Sommerfeldt.* Typesetting Captions with the caption Package*, February 2007.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/caption`*.*

[10] *Patrick W. Daly.* Natural Sciences Citations and References (Author-Year and Numerical Schemes)*, February 2009.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/natbib`*.*

[11] *Michael Downes and Barbara Beeton.* The amsart, amsproc, and amsbook document classes. *American Mathematical Society, August 2004.* `http://www.ctan.org/tex-archive/macros/latex/required/amslatex/classes`*.*

[12] *David Carlisle.* The longtable Package*, February 2004.* `http://www.ctan.org/tex-archive/macros/latex/required/tools`*.*

[13] *Martin Schröder.* The ragged2e Package*, March 2003.* `http://ctan.tug.org/tex-archive/macros/latex/contrib/ms`*.*

[14] *Leslie Lamport, Frank Mittelbach, and Johannes Braams.* Standard Document Classes for LaTeX version 2e*, 1997.* `http://ctan.tug.org/tex-archive/macros/latex/base`*.*

[15] *David Carlisle.* The dcolumn Package*, May 2001.* `http://ctan.tug.org/tex-archive/macros/required/tools`*.*

[16] *American Mathematical Society.* User's Guide for the amsmath Package (Version 2.0)*, February 2002.* `http://ctan.tug.org/tex-archive/macros/`

`latex/required/amslatex/math/amsldoc.pdf`.

[17] Boris Veytsman. LaTeX Support for Microsoft Georgia and ITC Franklin Gothic In Text and Math, *July 2009.* `http://ctan.tug.org/tex-archive/fonts/mathgifg/`.