# ISO/IEC TR 15942:2000-03 (E)

## Information technology - Programming languages - Guide for the use of Ada programming language in high integrity systems

## Contents

Page


1 Scope ..... 1
1.1 Within the scope ..... 1
1.2 Out of scope ..... 2

2 Verification Techniques ..... 2
2.1 Traceability ..... 2
2.2 Reviews ..... 3
2.3 Analysis ..... 3
2.3.1 Control Flow analysis ..... 4
2.3.2 Data Flow analysis ..... 4
2.3.3 Information Flow analysis ..... 4
2.3.4 Symbolic Execution ..... 4
2.3.5 Formal Code Verification ..... 5
2.3.6 Range Checking ..... 6
2.3.7 Stack Usage analysis ..... 6
2.3.8 Timing Analysis ..... 6
2.3.9 Other Memory Usage analysis ..... 6
2.3.10 Object Code Analysis ..... 7
2.4 Testing ..... 7
2.4.1 Principles ..... 7
2.4.2 Requirements-based Testing ..... 7
2.4.3 Structure-based Testing ..... 8
2.5 Use of Verification Techniques in this Technical Report ..... 8

3 General Language Issues ..... 9
3.1 Writing Verifiable Programs ..... 9
3.1.1 Language Rules to Achieve Predictability ..... 10
3.1.2 Language Rules to Allow Modelling ..... 10
3.1.3 Language Rules to Facilitate Testing ..... 11
3.1.4 Pragmatic Considerations ..... 12
3.1.5 Language Enhancements ..... 12
3.2 The Choice of Language ..... 13

4 Significance of Language Features for High Integrity ..... 14
4.1 Criteria for Assessment of Language Features ..... 14
4.2 How to use this Technical Report ..... 14

5 Assessment of Language Features ..... 15
5.1 Types with Static Attributes ..... 16
5.1.1 Evaluation ..... 17
5.1.2 Notes ..... 17
5.1.3 Guidance ..... 17
5.2 Declarations ..... 17
5.2.1 Evaluation ..... 18
5.2.2 Notes ..... 18
5.2.3 Guidance ..... 18
5.3 Names, including Scope and Visibility ..... 19
5.3.1 Evaluation ..... 19
5.3.2 Notes ..... 19
5.3.3 Guidance ..... 20
5.4 Expressions ..... 20

5.4.1 Evaluation ..... 21
5.4.2 Notes ..... 21
5.4.3 Guidance ..... 22
5.5 Statements ..... 22
5.5.1 Evaluation ..... 23
5.5.2 Notes ..... 23
5.5.3 Guidance ..... 23
5.6 Subprograms ..... 24
5.6.1 Evaluation ..... 24
5.6.2 Notes ..... 24
5.6.3 Guidance ..... 25
5.7 Packages (child and library) ..... 25
5.7.1 Evaluation ..... 26
5.7.2 Notes ..... 26
5.7.3 Guidance ..... 26
5.8 Arithmetic Types ..... 27
5.8.1 Evaluation ..... 27
5.8.2 Notes ..... 27
5.8.3 Guidance ..... 28
5.9 Low Level and Interfacing ..... 29
5.9.1 Evaluation ..... 30
5.9.2 Notes ..... 30
5.9.3 Guidance ..... 31
5.10 Generics ..... 31
5.10.1 Evaluation ..... 32
5.10.2 Notes ..... 32
5.10.3 Guidance ..... 33
5.11 Access Types and Types with Dynamic Attributes ..... 34
5.11.1 Evaluation ..... 34
5.11.2 Notes ..... 34
5.11.3 Guidance ..... 35
5.12 Exceptions ..... 35
5.12.1 Evaluation ..... 36
5.12.2 Notes ..... 36
5.12.3 Guidance ..... 36
5.13 Tasking ..... 37
5.13.1 Evaluation ..... 39
5.13.2 Notes ..... 39
5.13.3 Guidance ..... 39
5.14 Distribution ..... 40
5.14.1 Evaluation ..... 40
5.14.2 Notes ..... 40
5.14.3 Guidance ..... 40

6 Compilers and Run-time Systems ..... 40
6.1 Language issues ..... 41
6.2 Compiler Qualification ..... 41
6.3 Run-Time System ..... 42

7 References ..... 43
7.1 Applicable Documents ..... 43
7.2 Referenced Documents ..... 44