INTERNATIONAL STANDARD

ISO/IEC 23643

First edition
2020-06

Software and systems engineering — Capabilities of software safety and security verification tools

Ingénierie du logiciel et des systèmes — Capacités des outils de vérification de la sûreté et de la sécurité des logiciels

Reference number
ISO/IEC 23643:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **6**
5 Models for software safety and security verification tools ... **7**
6 Use cases of software safety and security verification tools ... **9**
6.1 General ... 9
6.2 Verification for low criticality software ... 10
6.3 Verification for medium criticality software ... 10
6.4 Verification for high criticality software ... 11
7 Entity relationship chart of software safety and security verification ... **12**
8 Categories, capabilities of and requirements for software safety and security verification tools ... **13**
8.1 General ... 13
8.2 Categories of software safety verification tools ... 13
8.2.1 General ... 13
8.2.2 Specification and refinement tools ... 13
8.2.3 Model checking tools ... 13
8.2.4 Program analysis tools ... 14
8.2.5 Proof tools ... 14
8.2.6 Monitoring tools ... 14
8.2.7 Programming rules checkers ... 14
8.3 Categories of software security verification tools ... 15
8.3.1 General ... 15
8.3.2 Vulnerability analysis tools ... 15
8.3.3 Security modeling tools ... 15
8.3.4 Threat modeling tools ... 15
8.4 Capabilities of software safety and security verification tools ... 15
8.5 Common requirements for safety and security verification tools ... 19
8.6 Requirements for specification and refinement tools ... 20
8.7 Requirements for model checking tools ... 20
8.8 Requirements for program analysis tools ... 21
8.9 Requirements for proof tools ... 21
8.10 Requirements for monitoring tools ... 22
8.11 Requirements for programming rules checking tools ... 22
8.12 Requirements for vulnerability analysis tools ... 22
8.13 Requirements for security modeling tools ... 23
8.14 Requirements for threat modeling tools ... 23
Annex A (informative) **Evaluation assurance levels of ISO/IEC 15408 common criteria** ... **24**
Annex B (informative) **How to use this document with ISO/IEC 20741** ... **28**
Bibliography ... **29**

© ISO/IEC 2020 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2020 – All rights reserved

Introduction

Since a few decades, the importance of software safety and security verification tools has increased for several reasons: 1) rapidly increasing complexity of software applications and systems, 2) increasing number of safety-critical systems through growing integration between software applications and systems (e.g. in critical infrastructures), 3) the rapid increase of the number of cyber threats, and 4) the urgent needs of safety in high and medium critical software-driven systems (e.g. transportation, energy production, Internet of Things (IoT), and general purpose Operating Systems and middleware). Additionally, the number of products and system development cases, where the origin of all software components to be used is not exactly known, even for open-source applications, is increasing and thus making safety and security verification and validation (V&V) essential.

This document restricts its point of view to software and excludes computing and any other hardware from the context. In these other domains, other V&V methods and tools are used.

It is important to realize that verification of safety and security of software does not necessarily verify the system safety and system security of a system using the software as a component. However, if a system consists of software components which are not verified, the safety and security of the system cannot be guaranteed at any level.

"Continuous everything", including continuous software development and thus versioning delivery, requires continuous software safety and security verification. At every new version, V&V needs to be redone. The popular "agile development processes" permit shorter development iterations and more frequent product delivery, and consequently this requires more frequent verification than traditional development approaches. Verification is needed during software development as well as during software maintenance, whenever safety or security of software can be endangered.

Validation answers the question "are we building the right product?"

Verification answers the question "are we building the product right?"

Software validation checks if the software product satisfies the intended use, such as defined in requirements and specifications. In other words (ISO/IEC 17029): "purpose of validation is to find out, whether a declared information (claim) is plausible". Software verification checks if the specifications and requirements are met either by running the software (testing) or by reviewing its artefacts (specification, model, or pseudo code). The latter can consist of animating or analyzing statically one of its artefacts. ISO/IEC 17029 defines that the "purpose of verification is to find out, whether a declared information (claim) is truthful". This document does not concern testing but animating and analyzing the artefacts, because "testing tools" is already well covered by and is the subject of ISO/IEC 30130.

This document is prepared as one of the series of single tool capabilities which are used with ISO/IEC 20741.

This document defines capabilities of and requirements for software safety and security verification tools.

This document is independent of the target application domains, as the languages, methods and associated tools are of general purpose, and can fit into different kinds of problems (e.g. functional specification languages can be used for any functional program).

© ISO/IEC 2020 – All rights reserved

Software and systems engineering — Capabilities of software safety and security verification tools

1 Scope

This document specifies requirements for the vendors and gives guidelines for both the users and the developers of software safety and security verification tools. The users of such tools include, but are not limited to, bodies performing verification and software developers who need to be aware and pay attention to safety and/or security of software. This document guides the verification tool vendors to provide as high-quality products as possible and helps the users to understand the capabilities and characteristics of verification tools.

This document introduces use cases for software safety and security verification tools and entity relationship model related to them. This document also introduces tool categories for software safety and security verification tools and gives category specific guidance and requirements for the tool vendors and developers.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
application domain
well-defined set of applications

3.2
capability
quality of being able to perform a given activity

[SOURCE: ISO 19439:2006, 3.5]

3.3
certificate
attestation document issued by an independent third-party certification body

[SOURCE: ISO 22222:2005, 3.2]

3.4
defect
fault, or deviation from the intended level of performance of a system or *software* (3.19)

© ISO/IEC 2020 – All rights reserved