IEC TR 63183

Edition 1.0 2019-12

TECHNICAL REPORT

colour inside

Guidance on error and warning messages for software used in radiotherapy

IEC TR 63183:2019-12(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TR 63183

Edition 1.0 2019-12

TECHNICAL REPORT

colour inside

Guidance on error and warning messages for software used in radiotherapy

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 11.040.60

ISBN 978-2-8322-7715-7

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 General guidance 8
5 Designing error message displays 8
5.1 Design systems to avoid the errors in the first place 8
5.2 Categorize messages 8
5.3 Consolidate reports and displayed error messages 9
5.4 Summary of main concepts 9
6 Message content usability guidelines 10
6.1 Basic structure 10
6.2 OPERATOR centred 10
6.3 Message clarity 10
6.4 Message action ability 12
6.5 Conciseness 12
6.6 Message specificity 12
6.7 Courteous 13
6.8 Use of error codes 13
7 Guidelines for the development process 13
8 Visual design guidelines 14
Annex A (informative) Checklist 15
Annex B (informative) Examples 16
Bibliography 23
Index of defined terms 24

Figure 1 – Example error message answering what happened, why and what to fix 10
Figure 2 – Example error message with unclear language on how to proceed 11
Figure 3 – Example error message with unfamiliar OPERATOR abbreviations 11
Figure 4 – Example error message implying the system thinks 11
Figure 5 – Example of an unhelpful error message 12
Figure 6 – Example error message showing error code 13
Figure B.1 – Example 1 16
Figure B.2 – Example 2 16
Figure B.3 – Example 3 17
Figure B.4 – Example 4 17
Figure B.5 – Example 5 17
Figure B.6 – Example 6 18
Figure B.7 – Example 7 18
Figure B.8 – Example 8 18
Figure B.9 – Example 9 19
Figure B.10 – Example 10 19

Figure B.11 – Example 11 20
Figure B.12 – Example 12 20
Figure B.13 – Example 13 20
Figure B.14 – Example 14 21
Figure B.15 – Example 15 21
Figure B.16 – Example 16 22
Figure B.17 – Example 17 22
Figure B.18 – Example 18 22

Table 1 – Replacing engineering language with language understandable for operators 10

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

GUIDANCE ON ERROR AND WARNING MESSAGES FOR SOFTWARE USED IN RADIOTHERAPY

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63183, which is a Technical Report, has been prepared by subcommittee 62C: Equipment for radiotherapy, nuclear medicine and radiation dosimetry, of IEC technical committee 62: Electrical equipment in medical practice.

The text of this Technical Report is based on the following documents:

Draft TR	Report on voting
62C/738/DTR	62C/741/RVDTR

Full information on the voting for the approval of this Technical Report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

In this document, the following print types are used:

– requirements and definitions: roman type;

– *test specifications: italic type*;

– informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type;

– TERMS DEFINED IN CLAUSE 3 OF IEC 60601-1, IN THIS DOCUMENT OR AS NOTED: SMALL CAPITALS.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document is intended to be read by persons involved in software development for RADIOTHERAPY and provides guidance on how to write relevant error messages shown to the clinical OPERATORS. This document is meant to provide examples within the RADIOTHERAPY domain and is not meant to replace IEC/ISO standards governing usability (for example, IEC 62366-1:2015). With the advent of more RADIOTHERAPY equipment being computer controlled, there has been a reported increase in the number of treatment delivery errors, some serious, occurring due to misunderstanding of the various error and warning messages shown to the OPERATOR during usage. Mistakes in interpretation are more likely to occur when error messages are written in technical language or are presented to the user without an OPERATOR-friendly explanation.

This problem is compounded by use of the following practices:

– message dialogs are designed from the program's technical point of view and not from the clinical OPERATOR'S point of view;

– message dialogs are optimized for engineering purposes with little input from end USERS;

– insufficient attention and resources are given to applying good practices for usability of message dialogs and careful review by clinical representatives.

In addition, the frequency of messages displayed by the many pieces of RADIOTHERAPY equipment to the OPERATOR can lead to "message overload". This increases the RISK that the OPERATOR will ignore critical information.

This document provides guidance via examples of common mistakes made when writing error messages to be displayed to the OPERATOR.

GUIDANCE ON ERROR AND WARNING MESSAGES FOR SOFTWARE USED IN RADIOTHERAPY

1 Scope

This document, which is a Technical Report, provides guidance on the usage and form of error or warning messages written for software used in RADIOTHERAPY. It does not replace any requirements existing in the safety standards but is meant to be used as a supplement to existing standards on usability by providing specific examples in the field of RADIOTHERAPY.

The two main goals of this document are

1) to present in a concise manner the best practices and design guidelines for good message dialogs, and
2) to illustrate these design guidelines with specific examples from the field of radiation oncology.

This document is intended to be read by the following MANUFACTURERS' employees and representatives:

– engineering department members including: software engineers, RISK managers, quality assurance engineers, technical writers, etc.;
– usability and human factors engineers;
– marketing representatives (product marketing, product managers, business analysts).

Throughout this document, unless specifically called out, these guidelines apply to all categories of messages summarily called error or warning messages (e.g. critical error, warning, system status, informational, routine interlock messages).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*
IEC 60601-1:2005/AMD1:2012

IEC 60601-2-1:—, *Medical electrical equipment – Part 2-1: Particular requirements for the basic safety and essential performance of electron accelerators in the range 1 MeV to 50 MeV*[1]

IEC TR 60788:2004, *Medical electrical equipment – Glossary of defined terms*

IEC 62366-1:2015, *Medical devices – Part 1: Application of usability engineering to medical devices*

[1] Fourth edition under preparation. Stage at the time of publication: IEC/AFDIS 60601-2-1:2019.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60601-1:2005 and IEC 60601-1:2005/AMD1:2012, IEC TR 60788:2004 and IEC 60601-2-1:—[2] apply.

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

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

4 General guidance

This document is meant to provide guidance to MANUFACTURERS of RADIOTHERAPY equipment on the frequency, terminology and content of error messages.

While systems should be designed to avoid errors, it is impossible to eliminate them completely. This does not mean however that error messages should be used to mitigate known workflow issues. When designing fault management systems,

- use analytical methods such as failure mode and effects analysis (FMEA) and fault tree analysis (FTA),
- consider use-case scenarios, and
- design them with a global view of system state, analysing local subsystem states to produce comprehensive information about error states.

5 Designing error message displays

5.1 Design systems to avoid the errors in the first place

Robust engineering is required to prevent errors from occurring, as this will reduce the number of error messages in the first place. For a system that already exists, subsequent software versions should be developed by engineers who are trained to analyse the existing errors and warnings and design systems in a way to prevent the OPERATOR from getting to the conditions that lead to these messages (a robust system will have fewer errors and fewer error messages).

Use scenarios should be considered when designing fault management systems. Different clinical workflows may use devices in different ways, depending on the options and flexibility of these devices. The fault management may be different for each scenario. Scenarios should also consider different clinical environments (large versus small, dedicated physics support versus part time physics support, academic versus community) because staff in these environments may respond to messages differently.

5.2 Categorize messages

Error messages should be triaged and different reporting mechanisms should be used to distinguish messages based on the severity of the error. For example, use log files for information users do not need to know right away and only use error messages and interlocks for errors that need to be addressed immediately.

Certain error messages may need to be included strictly for legal reasons. When such legal messages are displayed, they should appear in a format that prevents confusion with either of the two categories of error message listed above.

---

2 Fourth edition under preparation. Stage at the time of publication: IEC/AFDIS 60601-2-1:2019.

5.3 Consolidate reports and displayed error messages

User interfaces should be designed so as to increase the probability that error messages are read.

1) Consolidate error messages into a unified display. Systems with multiple monitors should be designed so that the user knows where to expect error messages to appear (for example on only a single monitor).
2) Collect multiple messages into a single report when it can be done safely instead of creating a sequential process of displaying multiple message boxes that tempt the user to click through the set without reading carefully and, hence, potentially missing important information.
3) Use log files for messages that do not need to be presented to the user but are still needed for troubleshooting.
4) Do not require the OPERATOR to acknowledge transient fault messages which merely state that an interlock has already been cleared.
5) Use icons that show the system state and allow the user to click on them to get more information. Icons should be designed to incorporate more than one indication of system state such as colour change along with graphic change.
6) When designing icons, care should be taken, where possible, to account for various OPERATOR differences such as colour blindness. When available, icons that already have internationally recognized status should be used instead of creating new ones.

The following should be avoided:

7) Allowing OPERATORS to quickly dismiss important messages.
8) Message fatigue. Message fatigue can cause OPERATORS to ignore important information that could lead to mistreatments. To prevent error messages and OPERATOR responses from becoming routine, it is important to consider this "fatigue" in the safety engineering aspects of system design. It is therefore suggested that FMEA and other analysis methods be applied to the design of error messages to consider the appropriate frequency and mode of error reporting.

While it is acknowledged that many error messages exist due to product liability concerns, how often things appear on the screen and lead to message fatigue, which causes the messages to be ignored, leading to compromised safety.

5.4 Summary of main concepts

- Transient error messages that require the OPERATOR to "acknowledge" an interlocked transient condition that had already cleared are an example of presenting unnecessary error messages. Minor interlocks that are automatically cleared by the control system should not require user acknowledgement. If the system is safe, the OPERATOR should be able to continue. All errors should be captured in a log file.
- To address the frequency of error message display, one shall consider the underlying design of fault management. Systems that have a more global view of their state should be able to collect information from individual devices that have only a local view, and analyse these local errors to determine the appropriate responses within the context that generated them (e.g. OPERATOR actions leading to the event, the clinical workflow where the actions took place, etc.). By going to a more global view, it might be possible to provide fewer and more meaningful error messages (rather than just reporting every local device fault).
- Systems should be analysed for fault hierarchies, determining different levels based on severity of the error, the expertise required to deal with the error and the appropriate authorization to recover from the error and proceed. Depending on the level, the display of the information should be different (e.g. passwords on alert messages may be required to proceed with the workflow, versus a log file for offline review).