IEC 62429

Edition 1.0 2007-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Reliability growth – Stress testing for early failures in unique complex systems

Croissance de fiabilité – Essais de contraintes pour révéler les défaillances précoces d'un système complexe et unique

IEC 62429:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62429

Edition 1.0 2007-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Reliability growth – Stress testing for early failures in unique complex systems

Croissance de fiabilité – Essais de contraintes pour révéler les défaillances précoces d'un système complexe et unique

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX W

ICS 03.120.01; 03.120.99

ISBN 2-8318-9427-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

RELIABILITY GROWTH – STRESS TESTING FOR EARLY FAILURES IN UNIQUE COMPLEX SYSTEMS

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

International Standard IEC 62429 has been prepared by IEC technical committee 56: Dependability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1232/FDIS	56/1249/RVD

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

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

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

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

RELIABILITY GROWTH – STRESS TESTING FOR EARLY FAILURES IN UNIQUE COMPLEX SYSTEMS

1 Scope

This International Standard gives guidance for reliability growth during final testing or acceptance testing of unique complex systems. It gives guidance on accelerated test conditions and criteria for stopping these tests. “Unique” means that no information exists on similar systems, and the small number of produced systems means that information deducted from the test has limited use for future production.

This standard concerns reliability growth of repairable complex systems consisting of hardware with embedded software. It can be used for describing the procedure for acceptance testing, "running-in", and to ensure that reliability of a delivered system is not compromised by coding errors, workmanship errors or manufacturing errors. It only covers the early failure period of the system life cycle and neither the constant failure period, nor the wear out failure period. It can also be used when a company wants to optimize the duration of internal production testing during manufacturing of prototypes, single systems or small series.

It is applicable mainly to large hardware/software systems, but does not cover large networks, for example telecommunications and power networks, since new parts of such systems cannot usually be isolated during the testing.

It does not cover software tested alone, but the methods can be used during testing of large embedded software programs in operational hardware, when simulated operating loads are used.

It addresses growth testing before or at delivery of a finished system. The testing can therefore take place at the manufacturer's or at the end user's premises.

If the user of a system performs reliability growth by a policy of updating hardware and software with improved versions, this standard can be used to guide the growth process.

This standard covers a wide field of applications, but is not applicable to health or safety aspects of systems.

This standard does not apply to systems that are covered by IEC 62279[39].

2 Normative references

The following referenced documents are indispensable for the application 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 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60605-2, *Equipment reliability testing – Part 2 Design of test cycles*

IEC 61163-1:2006, *Reliability stress screening – Part 1: Repairable assemblies manufactured in lots*

IEC 61163-2, *Reliability stress screening – Part 2: Electronic components*

IEC 61164, *Reliability growth – Statistical test and estimation methods*

IEC 61710, *Power law model – Goodness-of-fit and estimation methods*

3 Terms, definitions, abbreviations and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191, as well as the following, apply.

3.1.1
time compression
reducing test time by testing with higher use time than in the field

NOTE An example is testing a system that is used 8 h a day for 24 h a day.

3.1.2
accelerated test
test in which the applied stress level is chosen to exceed that stated in the reference conditions in order to shorten the time duration required to observe the stress response of the item, or to magnify the response in a given time duration

NOTE To be valid, an accelerated test should not alter the basic fault modes and failure mechanisms, or their relative prevalence.

[IEV 191-14-07]

3.1.3
(time) acceleration factor
ratio between the time durations necessary to obtain the same stated number of failures or degradations in two equal size samples, under two different sets of stress conditions involving the same failure mechanisms and fault modes and their relative prevalence.

NOTE One of the two sets of stress conditions should be a reference set.

[IEV 191-14-10]

3.1.4
execution time
time to perform a stated number of transactions

3.1.5
fault
state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

NOTE 1 A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEV 191-05-01]

NOTE 2 In English, the term "fault" is also used in the field of electric power systems with the meaning as given in IEV 604-02-01[42] 1; then, the corresponding term in French is "défaut".

NOTE 3 In this standard, the term "latent fault" is used to emphasize that the fault has not yet caused a failure.

NOTE 4 Software alone is deterministic. But this standard considers software embedded in hardware where the software can have latent faults relating to the hardware and the environment, e.g. insufficient protection against double keying, no checksum in communication, or no sanity check of input data or output data.

3.1.6
bug
popular name for a software latent fault

3.1.7
reliability indicator
non-functional parameter that points to a probable failure in a short time

3.1.8
success ratio test
test repeated a number of times of which all have to be passed without failures

3.1.9
system
set of interrelated or interacting elements

[ISO 9000:2005, 3.2.1] [41]

NOTE 1 In the context of dependability, a system will have

– a defined purpose expressed in terms of intended functions,

– stated conditions of operation/use, and

– defined boundaries.

NOTE 2 The structure of a system may be hierarchical [IEC 60300-1, 3.6] [43].

NOTE 3 For some systems, such as information technology products, data is an important part of the system elements.

[Future IEC 60300-3-15, modified] [44].

3.1.10
transaction
set of input parameters and preconditions selected from operating loads for the system

3.1.11
root cause analysis
activity to identify the cause of a fault or failure, so it can be removed by design or process changes

3.1.12
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE 1 An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

NOTE 2 The French term "erreur" may also designate a mistake (see IEV 191-05-25).

[IEV 191-05-24]

1 References in square brackets refer to the biblioraphy.

3.1.13
mistake
human error
human action that produces an unintended result

[IEV 191-05-25]

3.1.14
failure
termination of the ability of an item to perform a required function

NOTE 1 After failure the item has a fault

NOTE 2 "Failure" is an event, as distinguished from "fault", which is a state.

NOTE 3 This concept as defined does not apply to items consisting of software only

[IEV 191-04-01]

NOTE 4 Software alone is deterministic. But this standard considers software embedded in hardware where the software can have latent faults relating to the hardware and the environment, e.g. insufficient protection against double keying, no checksum in communication, or no validity check of input data or output data.

3.1.15
failure intensity
failure intensity; instantaneous failure intensity
$z(t)$

limit, if this exists, of the ratio of the mean number of failures of a repaired item in a time interval $(t, t + \Delta t)$, and the length of this interval, Δt, when the length of the time interval tends to zero

NOTE 1 The instantaneous failure intensity is expressed by the formula as

formula as

$$z(t) = \lim_{\Delta t \to 0+} \frac{E[N(t + \Delta t) - N(t)]}{\Delta t}$$

[IEV 191-12-04]

NOTE 2 To avoid confusion this standard will use “instantaneous failure intensity” since a system is repaired when it fails, and a latent fault is repaired (removed) when precipitated as a failure.

3.2 Abbreviations

CPU	Central processor unit
EMC	Electro magnetic compatibility
ESD	Electro static discharge
FMEA	Failure mode and effect analysis
MTBF	Mean operating time between failures
RAM	Random access memory

3.3 Symbols

C	total number of transactions
$D(t)$	the number of faults detected by time t
F_u	unacceptable number of failed transactions out of C transactions

i	fault number
M	probability that a system with an unacceptable reliability passes N tests without a failure
m	number of latent faults in the system
N	number of transactions to be performed without failure
p	unacceptable probability of failure per transaction
RCM $r(T_t)$	risk criterion metric for remaining latent faults at total test time T_t
r_c	the estimated number of remaining latent faults in the system
$r(T_t)$	remaining (undetected) latent faults predicted at accumulated test time T_t
s	number of test time intervals used in the Schneidewind model to estimate the model parameters
t	actual test time
t_{status}	test time at status
$T_{D(t)}$	the accumulated test time by which $D(t)$ faults were detected
T_i	the accumulated test time when fault i was detected T_{min}
T_{min}	the minimum test time that shall be accumulated by the system for 0 failures
T_t	accumulated test time measured in time units of the Schneidewind model
z	the acceptable instantaneous failure intensity
z_i	the instantaneous failure intensity of fault i
θ_i	cumulative mean operating time between failures (MTBF) when fault i was detected NOTE The term "cumulative MTBF" is used to be in line with other reliability growth models described in the literature. It is instructive in displaying a growth in reliability due to defect root cause elimination. The cumulative MTBF (θ_i) for each fault i is determined as $\theta_i = T_i / i$.
α	empirical constant in the Schneidewind model – failure intensity at test time = 0
β	empirical constant in the Schneidewind model – proportionality constant for failure intensity over time – Unit: $(\text{time})^{-1}$
δ	the probability of no failure occurring by T_{min} for a given acceptable instantaneous failure intensity

4 General

This standard is one of a series of standards under the application guide IEC 61014 [34].

This standard applies to large hardware-software systems when tested using a simulated operating load. Therefore, it is not known during the test if a failure is caused by hardware, software, operating load, or a combination of these. A failure may be caused by a hardware failure, e.g. a random access memory (RAM) failure, a change of timing causing data collision, or an electromagnetic disturbance, changing data transmitted. The failure may also be caused by a software latent fault or by illegal data. How the failed item is repaired or the software is changed is, for this standard, only relevant to the extent that it influences the test decisions, e.g. through the assumptions of the statistical model.

Nearly all modern systems contain embedded software. The software is typically tested on development hardware using transactions derived from the system specifications. Often the software is finished late so that the time for testing the software in the actual hardware is limited. It is usually not acceptable that the customer is the first to operate the software in the real hardware. Therefore, there is a need for a standard to guide testing and reliability growth of hardware with the embedded software.

With hardware, it is assumed that early failures are caused by a latent fault in the hardware. Depending on the stress type and stress level, these latent faults can be precipitated into permanent or intermittent failures after some time. An example could be a crack in a component. Under dry operating conditions without vibration or shocks, the latent fault may remain a latent fault. But under moist operating conditions, moisture and contaminants may penetrate the crack and cause corrosion, ending in a permanent fault. Similarly, vibration or shock can cause crack propagation that may cause a permanent fault after some time.

Software alone is deterministic. This means that a latent fault in the software (commonly called a software bug) will not result in a failure until the part of the code containing the latent fault is activated. The moment when this occurs depend on the operating conditions (e.g. input parameters and the internal states of the program, e.g. memory content). Therefore, there is a similarity between hardware latent faults and software latent faults. The software latent fault, once activated, may cause a permanent fault but will often only cause an intermittent failure.

Logical failures are systematic (i.e. they can be reproduced at will once the trigger for the associated fault is known). Since the trigger for any latent fault is encountered at random in the operating environment of the system, logical failures are observed as a stochastic process. Therefore, the usual measures of reliability can be applied (probability of time to next failure, failure intensity, etc.) Reliability growth will normally occur as latent faults are removed.

In this standard the term "latent fault" will therefore be used to cover weaknesses in hardware as well as bugs in software [10].

A failure caused by a combination of hardware and software could be, for example, that a hardware latent fault causes insufficient cooling of a component. The temperature rise changes the time delays in the circuit, causing data collision that results in a software failure. Another combination could be that a hardware design error causes insufficient shielding of signal wires. The increased level of electromagnetic noise corrupts the data in the signal wires causing a software failure, given that the software does not have an error correction feature, and the operating environment has a high electromagnetic noise level.

This standard covers repairable systems that are produced in a very small number of copies, so that experience from tests of previous similar systems is limited or non-existent. It can be used when a manufacturer wants to optimize the duration of internal acceptance testing and running-in. It addresses growth testing before or at delivery of a finished system. The testing can therefore take place at the manufacturer's or at the end user's premises. It can also be used when a company wants to optimize the duration of final production testing during manufacturing of single items, small series or during testing of a prototype.

It can also be used by the owner of only one, or a few, large systems to improve those systems only. If the user of a system performs reliability growth by a policy of updating hardware and software with improved versions, this standard can be used to control the growth process.

This standard does not cover software alone, but it can be used when embedded software is tested in a hardware system using test strategies that give a diminishing number of failures as a function of test time, for example a software test with simulated operational load. The methods described are well suited to test and improve the robustness of a software program against transients and disturbances caused by the operational load and by the hardware system. It addresses large hardware/software systems, but does not cover large networks, for example, telecommunications and power networks, since the new parts of these are difficult to isolate during the testing process.

Reliability growth is a method aimed at improving quality by identifying and removing latent faults, but should not be used as the primary means of achieving the intended quality and reliability of the systems produced. Large systems are often produced in a small number of copies. Often only one or a few systems are produced. The remaining latent faults introduced through the design and manufacturing processes therefore shall be identified via growth testing of the finished system. However, an appropriate process control should be used and preventive methods such as an FMEA process (see IEC 60812) [33], fault tree analysis (see IEC 61025 [35]) and design reviews (see IEC 61160 [37]) should be used to reduce the number of latent faults in the produced system(s). Further, the manufacturing processes and assembly processes should be controlled, for example using statistical process control.

In some cases, it may be possible to divide a large system into a number of similar modules on which the methods of IEC 61163-1 can be used. The similar modules are then regarded as a lot consisting of similar items. This will cover latent faults in the modules but not failures caused by the interaction of the modules and interactions between the modules and the embedded software.

The failures caused by the interaction between the modules can be found only by growth testing the finished system. In modern systems, many failures are caused by an interaction between hardware and software. These failures cannot be found before the whole system is finished and functional. When the prototype is the only system produced, prototype testing and growth testing merge into one activity.

This standard covers only the early failure period of the system life cycle. This means that it does not cover the random failure period or the wear out failure period of the bathtub curve, as illustrated in Figure 1.

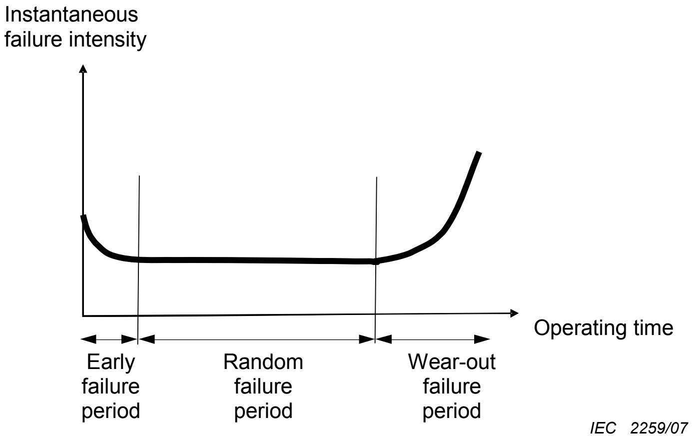

Figure 1 – The bathtub curve

NOTE This standard applies to the early failure period. Due to increased stress or time compression, this part of the operating time may be covered by a shorter period of growth testing.

When planning a reliability growth testing process, the decision makers should carefully consider time and cost against the performance of the system including the risks and costs associated with early failures in the system after delivery. All failures identified during testing shall be carefully analysed in order to find the root cause, and to ensure that the experiences are used to prevent similar problems in other systems. The finished system(s) shall be repaired or updated, re-tested for normal operation, and the system documentation shall be updated as appropriate.

If discrepancies arise between this standard and the relevant contract or specification(s), the latter shall apply.

5 Planning and performing a reliability growth test

5.1 Step 1 – Should a reliability growth test be used?

A reliability growth test is relevant in the following cases:

- the savings in costs due to reduction of early failures is larger than the cost of the test including the necessary monitoring and test equipment;
- where no previous test data exist for the whole system, since only one or a few systems have been produced, or only one system requires testing;
- where early failures are expected due to latent faults introduced in the assembly processes and the components or due to tolerance interference between components in the system;
- where relevant early failures in modules and components should be screened out by reliability stress screening before the start of the system test (see IEC 61163-1 and IEC 61163-2);
- where early failures are expected due to interaction between the hardware of the system and the embedded software;
- when using a test strategy where reliability growth is expected, i.e. the failure intensity should decrease with test time;
- when tests are performed using simulated operating loads, when possible higher than average loads can be used, and where relevant abnormal loads (noisy data, illegal data or overload conditions) can be added; or
- where possible hardware latent faults are precipitated into permanent or intermittent failures by increasing environmental stresses, i.e. by increasing temperature, temperature changes, vibration, shock, etc.

5.2 Step 2 – Failure definitions and data collection

A practical approach is to list the system requirements and check which requirements should be monitored. Then determine how the system can be monitored during the test. The test specification shall define relevant and non-relevant failures.

Relevant failures are sudden failures (function missing) as well as gradual failures (degradation). Further software related failures, i.e. no answer, wrong answer, system locked or excessive response time, should be defined. The failures may be caused by hardware, the embedded software or the interaction between the hardware and the software, e.g. shift in time delays causing data collision or electromagnetic noise changing data.

Non-relevant failures are failures caused by the test equipment, the monitoring equipment or by the test operators. If robustness testing of the system against human errors (mistakes made by the operator) is to be included in the growth test, these errors shall be defined as relevant failures.

If possible, the system should be monitored continuously for function and performance. To the extent that this is not possible, a functional test, including check of function of redundant units, should be made at fixed intervals. When stress cycles are used, the system should be checked for function after each cycle. The status of redundancy and automatic reconfiguration as well as other relevant internal system parameters should be monitored during the testing.

System changes such as replacing a module or switching operating modes shall also be recorded. A practical procedure is to report all events, e.g. start, stop, failure, upgrade, change of configuration, i.e. operating mode, etc., in the test protocol. It is recommended to