H.2.19.1
Abraham test
a specific form of a variable memory pattern test in which all stuck-at and coupling faults between memory cells are identified

The number of operations required to perform the entire memory test is about 30 n, where n is the number of cells in the memory. The test can be made transparent for use during the operating cycle, by partitioning the memory and testing each partition in different time segments.

Abraham, J.A.; Thatte, S.M.; "Fault coverage of test programs for a microprocessor", Proceedings of the IEEE Test Conference 1979, pp 18-22.

H.2.19.2
GALPAT memory test
a fault/error control technique in which a single cell in a field of uniformly written memory cells is inversely written, after which the remaining memory under test is inspected. After each read operation to one of the remaining cells in the field, the inversely written cell is also inspected and read. This process is repeated for all memory cells under test. A second test is then performed as above on the same memory range without inverse writing to the test cell

The test can be made transparent for use during the operating cycle, by partitioning the memory and testing each partition in different time segments (see transparent GALPAT test).

H.2.19.2.1
transparent GALPAT test
a GALPAT memory test in which first a signature word is formed representing the content of the memory range to be tested and this word is saved. The cell to be tested is inversely written and the test is performed as above. However, the remaining cells are not inspected individually, but by formation of and comparison to a second signature word. A second test is then performed as above by inversely writing the previously inverted value to the test cell

This technique recognizes all static bit errors as well as errors in interfaces between memory cells.

checkerboard memory test (see H.2.19.6.1)

H.2.19.3 Checksum

H.2.19.3.1
modified checksum
a fault/error control technique in which a single word representing the contents of all words in memory is generated and saved. During self test, a checksum is formed from the same algorithm and compared with the saved checksum

This technique recognizes all the odd errors and some of the even errors.

H.2.19.3.2
multiple checksum
a fault/error control technique in which a separate words representing the contents of the memory areas to be tested are generated and saved. During self test, a checksum is formed from the same algorithm and compared with the saved checksum for that area

This technique recognizes all the odd errors and some of the even errors.

H.2.19.4 Cyclic redundancy check (CRC)

H.2.19.4.1
CRC – single word
a fault/error control technique in which a single word is generated to represent the contents of memory. During self test the same algorithm is used to generate another signature word which is compared with the saved word

This technique recognizes all one-bit, and a high percentage of multi-bit, errors.

H.2.19.4.2
CRC – double word
a fault/error control technique in which at least two words are generated to represent the contents of memory. During self test the same algorithm is used to generate the same number of signature words which are compared with the saved words

This technique can recognize one-bit and multi-bit errors with a greater accuracy than in CRC – single word.

marching memory test (see H.2.19.6.2)

modified checksum (see H.2.19.3.1)

multiple checksum (see H.2.19.3.2)

H.2.19.5
redundant memory with comparison
a structure in which the safety-related contents of memory are stored twice in different format in separate areas so that they can be compared for error control

H.2.19.6
static memory test
a fault/error control technique which is intended to detect only static errors

H.2.19.6.1
checkerboard memory test
a static memory test in which a checkerboard pattern of zeros and ones is written to the memory area under test and the cells are inspected in pairs. The address of the first cell in each pair is variable and the address of the second cell is derived from a bit inversion of the first address. In the first inspection, the variable address is first incremented to the end of the address space of the memory and then decremented to its original value. The test is repeated with the checkerboard pattern inversed

H.2.19.6.2
marching memory test
a static memory test in which data is written to the memory area under test as in normal operation. Every cell is then inspected in ascending order and a bit inversion performed on the contents. The inspection and bit inversion are then repeated in descending order. Then this process is repeated after first performing a bit inversion on all the memory cells under test

transparent GALPAT test (see H.2.19.2.1)

H.2.19.7
walkpat memory test
a fault/error control technique in which a standard data pattern is written to the memory area under test as in normal operation. A bit inversion is performed on the first cell and the remaining memory area is inspected. Then the first cell is again inverted and the memory

inspected. This process is repeated for all memory cells under test. A second test is conducted by performing a bit inversion of all cells in memory under test and proceeding as above

This technique recognizes all static bit errors as well as errors in interfaces between memory cells.

H.2.19.8 Word protection

H.2.19.8.1
word protection with multi-bit redundancy
a fault/error control technique in which redundant bits are generated and saved for each word in the memory area under test. As each word is read, a parity check is conducted

An example is a hamming code which recognizes all one and two bit errors as well as some three bit and multi-bit errors.

H.2.19.8.2
word protection with single bit redundancy
a fault/error control technique in which a single bit is added to each word in the memory area under test and saved, creating either even parity or odd parity. As each word is read, a parity check is conducted

This technique recognizes all odd bit errors.

H.2.20 Definitions of software terminology – General

H.2.20.1
common mode error
error(s) in a dual channel or other redundant structure such that each channel or structure is affected simultaneously and in the same manner

H.2.20.2
failure modes and effects analysis (FMEA)
analytical technique in which the failure modes of each hardware component are identified and examined for their effects on the safety-related functions of the control

H.2.20.3
independent
not being adversely influenced by the control data flow and not being impaired by failure of other control functions, or by common mode effects

H.2.20.4
invariable memory
memory ranges in a processor system containing data which is not intended to vary during programme execution

Invariable memory may include RAM construction where the data is not intended to vary during programme execution.

H.2.20.5
variable memory
memory ranges in a processor system containing data which is intended to vary during programme execution

H.2.21 Void

H.2.22 Definitions relating to classes of control functions

For the evaluation of protective measures for fault tolerance and avoidance of hazards it is necessary to classify control functions with regard to their fault behaviour.

At the classification of control functions their integration into the complete safety concept of the appliance shall be taken into account.

NOTE A control function consists of the entire loop beginning with the sensing means through the processing circuitry (hardware and software if used) and including the actuator drive.

For the purpose of evaluating the design of a control function, present requirements recognise three distinct classes:

H.2.22.1
class A control function
control functions which are not intended to be relied upon for the safety of the application

NOTE Examples are: room thermostats, temperature control.

H.2.22.2
class B control function
control functions which are intended to prevent an unsafe state of the appliance. Failure of the control function will not lead directly to a hazardous situation

NOTE Examples are: thermal limiter, pressure limiter.

H.2.22.3
class C control function
control functions which are intended to prevent special hazards such as explosion or whose failure could directly cause a hazard in the appliance

NOTE Examples are: burner control systems, thermal cut-outs for closed water systems (without vent protection).

H.2.23 Definitions relating to functional safety

H.2.23.1
fault tolerating time

time between the occurrence of a fault and the shut down of the controlled equipment, which is tolerated by the application without creating a hazardous situation

NOTE Actions other than shut down of the controlled equipment are possible if they can be shown to prevent hazardous situations.

H.2.23.2
fault reaction time
time between the occurrence of a fault and the point where the control has reached a defined state

H.2.23.3
defined state
state of a control with the following characterisation:

a) the control passively assumes a state in which the output terminals ensure a safe situation under all circumstances. When the cause of the transition to defined state is lifted, the application should start-up in accordance with the appropriate requirements; or

b) the control actively executes a protective action, within the time as specified in the relevant part 2, causing a shut down , or preventing an unsafe condition; or

c) the control remains in operation, continuing to satisfy all safety related functional requirements

H.2.23.4
complex electronics
denote assemblies which use electronic components with the following characteristics:

a) the component provides more than one functional output;

b) it is impractical or impossible to represent the failure mode of such a component by stuck-at and cross-links at the pins or by other failure modes which are described in Table H.21 (H.27.1 of the previous edition)

H.2.23.5
reset
action which provides reset from safe-state to allow the system to attempt a restart

H.2.23.6 Void

H.2.23.7
degradation (of performance)
undesired departure in the operational performance of any device, equipment or system from its intended performance

[IEC 161-01-19:1990]

NOTE The term "degradation" can apply to temporary or permanent failure.

H.2.23.8 Void

H.2.23.9
harm
physical injury or damage to health of people, or damage to property or the environment

[3.3 of ISO/IEC Guide 51:1999]

H.2.23.10
hazard
potential source of harm

[3.5 of ISO/IEC Guide 51:1999]

H.2.23.11
risk
combination of the probability of occurrence of harm and the severity of that harm

[3.2 of ISO/IEC Guide 51:1999]

H.2.23.12
reasonably foreseeable misuse
use of a product, process or service under conditions or for purposes not intended by the supplier, but which may happen, induced by the design of the product in combination with, or as result of, common human behaviour

[3.14 of ISO/IEC Guide 51:1999, modified]

H.2.23.13
functional safety
safety related to the application which depends on the correct functioning of the safety-related control

H.4 General notes on tests

H.4.1 Conditions of test

H.4.1.4 *Addition:*

For electronic controls, the tests of Clauses H.25, H.26 and H.27 are carried out before the tests of Clause 21.

Additional subclauses:

H.4.1.9 *Electronic controls shall be tested as electrical controls, unless otherwise specified.*

H.4.1.10 *When conducting the test sequence for electronic controls, care shall be taken that the results of a test are not influenced adversely by any preceding testing of the sample unless specifically required by the standard. It may be necessary to replace that sample, or parts thereof, or to use an additional sample.*

The number of samples should be kept to the minimum by an evaluation of the relevant circuits.

H.4.1.11 *Except for the test specified in Clause H.26, care shall be taken that the supply is free of such perturbations from external sources as may influence the results of the tests on electronic controls.*

H.6 Classification

H.6.4 According to features of automatic action

H.6.4.3 *Additional subclause:*

H.6.4.3.13 – electronic disconnection on operation (Type 1.Y – 2.Y)

H.6.9 According to circuit disconnection or interruption

Addition:

H.6.9.5 – electronic disconnection

H.6.18 According to classes of control functions (see Table 1 (7.2 of the previous edition), requirement 92)

H.6.18.1 – Control of class A control functions

H.6.18.2 – Control of class B control functions

H.6.18.3 – Control of class C control functions

H.7 Information

Additional items to Table 1 (7.2 of the previous edition) [12)]

Information	Clause or subclause	Method
Modification: 36 Limits of activating quantity for any sensing element over which micro-disconnection or electronic disconnection is secure	11.3.2, H.11.4.16, H.17.14, H.18.1.5, H.27.1.1, H.28	X
Additional items to Table 1 (7.2 of the previous edition): 52 The minimum parameters of any heat dissipator (e.g. heat sink) not provided with an electronic control but essential to its correct operation	14	D
53 Type of output waveform if other than sinusoidal	H.25	X
54 Details of the leakage current waveform produced after failure of the basic insulation	H.27	X
55 The relevant parameters of those electronic devices or other circuit components considered as unlikely to fail (see paragraph 1 of H.27.1.1.4)	H.27	X
56 Type of output waveform(s) produced after failure of an electronic device or other circuit component (see item g) of H.27.1.1.3)	H.27	X
57 The effect on controlled output(s) after electronic circuit component failure if relevant (item c) of H.27.1.1.3)	H.27	X
58a For integrated and incorporated electronic controls, if any protection against mains borne perturbations, magnetic and electromagnetic disturbances is claimed, which of the tests of Clause H.26 shall be performed and the effect on controlled output(s) and function after a failure to operate as a result of each test	H.26.2 H.26.15	X
58b For other than integrated and incorporated electronic controls, the effect on controlled output(s) and function after a failure to operate as a result of the tests of Clause H.26	H.26.2 H.26.15	X
59 Any component on which reliance is placed for electronic disconnection which is disconnected as required by Note 15 to Table 12 (13.2 of the previous edition)	13.2 H.27.1	X
60 Category (surge immunity)	H.26.8.2 H.26.10.4	X
66 Software sequence documentation [12) 13) 15) 18)]	H.11.12.2.9	X
67 Programme documentation [12) 14) 18)]	H.11.12.2.9 H.11.12.2.12	X
68 Software fault analysis [12) 15) 18)]	H.11.12 H.27.1.1.4	X
69 Software class(es) and structure [17)]	H.11.12.2 H.11.12.3 H.27.1.2.2.1 H.27.1.2.3.1	D
70 Analytical measures and fault/error control techniques employed [12) 16)]	H.11.12.1.2 H.11.12.2.2 H.11.12.2.4	X
71 Software fault/error detection time(s) for controls with software classes B or C [12) 19)]	H.2.17.10 H.11.12.2.6	X
72 Control response(s) in case of detected fault/error [12)]	H.11.12.2.7	X
73 Controls subjected to a second fault analysis and declared condition as a result of the second fault	H.27.1.2.3	X
74 External load and emission control measures to be used for test purposes	H.23.1.1	X
91 Fault reaction time	H.2.23.2 H.27.1.2.2.2 H.27.1.2.2.3 H.27.1.2.3.2 H.27.1.2.3.3 H.27.1.2.4.2 H.27.1.2.4.3	X

Additional items to Table 1 (7.2 of the previous edition) (concluded)

92 Class or classes of control function(s)	H.6.18 H.27.1.2.2 H.27.1.2.3	X

[12] For controls declared as entirely Class A, the requirements 66, 67, 68, 70, 71 and 72 are exempted. For controls with software classes B or C, information shall be provided only for the safety-related segments of the software. Information on the non-safety related segments shall be sufficient to establish that they do not influence the safety-related segments.

[13] The software sequence shall be documented and, together with the operating sequence of Table 1 (7.2 of the previous edition) requirement 46, shall include a description of the control system philosophy, the control flow, data flow and the timings.

[14] Programming documentation shall be supplied in a programming design language declared by the manufacturer.

[15] Safety-related data and safety-related segments of the software sequence, the malfunction of which could result in non-compliance with the requirements of 17, 25, 26 and 27, shall be identified. This identification shall include the operating sequence and may, for example, take the form of a fault tree analysis which shall include those fault/errors of table H.1 (H.11.12.7 of the previous edition) which could result in non-compliance. The software fault analysis shall be related to the hardware fault analysis in H.27.

[16] Measures to be declared are those chosen by the manufacturer from the requirements of H.11.12.1.2 to H.11.12.2.4 inclusive.

[17] Within a control, different software classes may apply to different control functions. Examples of control functions that may include software classes A to C are as follows:

Class A

Examples are room thermostats, humidity controls, lighting controls, timers and time switches.

Class B

An example is a thermal cut-outs

Class C

Examples are automatic burner controls and thermal cut-outs for closed water heater systems (unvented).

[18] Examples of other information which may be suitable for inclusion in the documentation required by notes [12] to [17] are:

Original software system specification, for example:

Functional specification, including procedure for restart on loss of supply

Module design, including description of equipment interfaces, and description of user interfaces

Detailed design, including description of use of memory

Code listing, including programming language identification, comments and listing of subroutines

Test specification

Manuals for installation, use and/or maintenance

[19] This can be expressed as a time following the execution of a specific software segment.

H.8 Protection against electric shock

H.8.1 General requirements

Additional subclauses:

H.8.1.10 Accessible parts shall not be considered as hazardous live parts if separated from the supply by protective impedance.

H.8.1.10.1 When protective impedance is used, the current between the part or parts and either pole of the supply source shall not exceed 0,7 mA (peak value) a.c. or 2 mA d.c.;

– for frequencies exceeding 1 kHz, the limit of 0,7 mA (peak value) is multiplied by the value of the frequency in kHz but shall not exceed 70 mA (peak value);
– for voltages over 42,4 V (peak value) and up to and including 450 V (peak value) the capacitance shall not exceed 0,1 μF;
– for voltages over 450 V (peak value) and up to and including 15 kV (peak value) the product of the capacitance in microfarads times the potential in volts shall not exceed 45 μC;
– for voltages over 15 kV (peak value) the product of the capacitance in microfarads times the square of the potential in volts shall not exceed 350 μJ.

Compliance is checked by measurement.

Voltages and currents are measured between a single accessible part (or any combination of such parts) and either pole of the supply source.

The measuring circuit shall have a total impedance of (1 750 ± 250) Ω and be shunted by a capacitor such that the time constant of the circuit is (225 ± 15) μs.

Details of a suitable circuit for measuring leakage currents are given in Annex E.

The measuring circuit shall have an accuracy of within 5 % for all frequencies in the range of 20 Hz to 5 kHz. For frequencies above 5 kHz, alternative methods of measurement are required.

H.11 Constructional requirements

H.11.2 Protection against electric shock

Additional subclauses:

H.11.2.5 Protective impedance shall consist of two or more impedance components of equivalent resistance values in series, which are connected between live parts and accessible parts. It shall consist of components in which the probability of a reduction in impedance during life can be ignored and the possibility of a short circuit is negligible.

Such components are resistors pointed out in Table H.21 (H.27.1 of the previous edition), Note 13.

Alternatively, the resistors shall comply with the requirements of 14.1 of IEC 60065.

Compliance is checked by

a) open-circuiting each impedance component in turn;

b) short-circuiting of those impedance components which are likely to fail by a short circuit (according to Clause H.27);

c) applying a fault condition according to Clause H.27 to any part of the circuit which might influence the maximum leakage current with the protective impedance intact.

Operation of a protective device or loss of one pole of the supply shall also be considered as faults.

Under these conditions, the equipment shall still comply with the requirements of H.8.1.10.

H.11.4 Actions

Additional subclauses:

H.11.4.16 Type 1.Y or 2.Y action shall operate to provide electronic disconnection.

Compliance is checked by the tests of this subclause.

H.11.4.16.1 The test is carried out with the control connected to its declared maximum load, supplied with rated voltage, and at temperature T_{max}.

H.11.4.16.2 The current through the electronic disconnection shall not exceed 5 mA or 10 % of the rated current, whichever is the lower.

H.11.12 Controls using software

Controls using software shall be so constructed that the software does not impair control compliance with the requirements of this standard.

Compliance is checked by the tests for electronic controls in this standard, by inspection according to the requirements of this subclause and by examination of the documentation required in items 66 to 72 inclusive of Table 1 (7.2 of the previous edition).

H.11.12.1 to **H.11.12.3** inclusive are only applicable to control functions using software class B or class C.

H.11.12.1 Requirements for the architecture

H.11.12.1.1 Control functions with software class B or C shall use measures to control and avoid software-related faults/errors in safety-related data and safety-related segments of the software, as detailed in H.11.12.1.2 to H.11.12.3 inclusive.

H.11.12.1.2 Control functions with software class C shall have one of the following structures:

– single channel with periodic self-test and monitoring (H.2.16.7);

– dual channel (homogenous) with comparison (H.2.16.3);

– dual channel (diverse) with comparison (H.2.16.2).

Comparison between dual channel structures may be performed:

– by the use of a comparator (H.2.18.3) or

– by reciprocal comparison (H.2.18.15).