IEC TR 63164-2

Edition 1.0 2020-07

TECHNICAL REPORT

Reliability of industrial automation devices and systems – Part 2: System reliability

IEC TR 63164-2:2020-07 (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 It also gives information on projects, replaced and withdrawn publications.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 63164-2

Edition 1.0 2020-07

TECHNICAL REPORT

Reliability of industrial automation devices and systems – Part 2: System reliability

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040

ISBN 978-2-8322-8663-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

RELIABILITY OF INDUSTRIAL AUTOMATION DEVICES AND SYSTEMS –

Part 2: System reliability

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 63164-2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

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

Enquiry draft	Report on voting
65/771/DTR	65/796/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.

A list of all parts in the IEC 63164 series, published under the general title *Reliability of industrial automation devices and systems*, can be found on the IEC website.

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.

INTRODUCTION

Under the background of Smart Manufacturing, new production modes such as mass customization based on interconnected factories require real-time interconnection, frequent switching and integration across different levels. Therefore, reliability is an important requirement for automation systems in factories. Reliability data of automation systems is the basis for maintenance planning e.g. stock-keeping of spare parts of a production line. An automation system usually consists of several different devices or machines that are used in series, parallel or mixed. This technical report gives guidance for system integrator on how to evaluate the reliability of such entire systems.

This report is the second part of the series. This part concentrates on calculation of failure rates or reliability values for systems based on failure rates or reliability values of single devices depending on the structure of the system. This is necessary for system integrators or designers to be able to calculate the reliability of an entire system from the reliability values of individual devices (see IEC TS 63164-1).

Parts within IEC 63164 series are:

Part 1: Assurance of automation devices reliability data and specification of their source

Part 2: System reliability

Future parts may include following subjects:

– collecting reliability data for automation devices in the field;
– user guide.

RELIABILITY OF INDUSTRIAL AUTOMATION DEVICES AND SYSTEMS –

Part 2: System reliability

1 Scope

This part of IEC 63164 provides guidance on the calculation of reliability data of automation systems which can be simplified as series, parallel or mixed structure based on reliability data of single devices and/or sub-systems, and on the form to present the data.

NOTE This procedure is only targeted to the reliability of automation systems, but not systems that embed automation systems, e.g. process plant.

Reliability is included in dependability, and this document is mainly focused on random hardware failures that affect reliability. Dependability is used as a collective term for the time-related quality characteristics of an item and additionally includes availability, recoverability, maintainability, maintenance support performance, and, in some cases, other characteristics such as durability, safety and security, which are all not in the scope of this Technical Report.

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.

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 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:

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

3.1.1
automation system
DCS- or PLC-based system for the monitoring and controlling of production facilities in the process industry, including control systems based on fieldbus technologies

Note 1 to entry: Whenever “system” is mentioned in this document, it means “automation system”.

[SOURCE: IEC 62381:2012, 3.1.1, modified – Note 1 to entry has been added.]

3.1.2
B_{10} threshold
time until 10 % of the components fail

Note 1 to entry: The applicable time interval is dependent on the nature and application of the asset and can be elapsed time, operating hours, number of cycles, etc.

Note 2 to entry: For this document, an average failure rate is calculated from the B_{10} threshold by dividing 10 % with the B_{10} threshold in hours. The influence of infant mortality is neglected and increasing failure rate is assumed only significant after B_{10}.

Note 3 to entry: Once the B_{10} threshold is reached, the failure rate is assumed unacceptable for pneumatic and electromechanical components.

3.1.3
dependability
ability to perform as and when required

Note 1 to entry: Dependability includes availability (192-01-23), reliability (192-01-24), recoverability (192-01-25), maintainability (192-01-27), and maintenance support performance (192-01-29), and in some cases, other characteristics such as durability (192-01-21), safety and security.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-192:2015, 192-01-22]

3.1.4
failure rate
λ
limit, if it exists, of the quotient of the conditional probability that the failure of a non-repairable item occurs within time interval (t, t + Δt) by Δt, when Δt tends to zero, given that failure has not occurred within time interval (0, t)

Note 1 to entry: See IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms, for more detail.

[SOURCE: IEC 60050-192:2015, 192-05-06, modified – The first preferred term "instantaneous failure rate", formula and Note 2 to entry have been deleted]

3.1.5
mean operating time between failures
MTBF
expectation of the duration of the operating time between failures

Note 1 to entry: Mean operating time between failures should only be applied to repairable items. For non-repairable items, see mean operating time to failure (192-05-11).

[SOURCE: IEC 60050-192:2015, 192-05-13, modified – The last preferred term "MOTBF" has been deleted]

3.1.6
mean operating time to failure
MTTF
expectation of the operating time to failure

Note 1 to entry: In the case of non-repairable items with an exponential distribution of operating times to failure (i.e. a constant failure rate) the MTTF is numerically equal to the reciprocal of the failure rate. This is also true for repairable items if after restoration they can be considered to be "as-good-as-new".

[SOURCE: IEC 60050-192:2015, 192-05-11, modified – Note 2 has been deleted]

3.1.7
mean time to restoration
MTTR
expectation of the time to restoration

Note 1 to entry: IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) defined the term ”mean time to recovery” as a synonym, but restoration and recovery are not synonyms.

[SOURCE: IEC 60050-192:2015, 192-07-23]

3.1.8
mission time
T_M
period of time covering the intended use

Note 1 to entry: For complex system with maintenance of components, the mission time of system can be longer than the mission time of individual components of the system.

[SOURCE: ISO 13849-1:2015, 3.1.28, modified – "of an SRP/CS" has been deleted and the note to entry has been added]

3.1.9
random hardware failure
failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – The notes have been deleted]

3.1.10
reliability
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – Note 3 to entry has been deleted]

3.1.11
systematic failure
failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

– the safety requirements specification;

– the design, manufacture, installation, operation of the hardware;

– the design, implementation, etc. of the software.

Note 4 to entry: In this document, failures in a safety-related system are categorized as random hardware failures (see 3.1.9) or systematic failures.

[SOURCE: IEC 61508-4:2010, 3.6.6]

3.1.12
useful life
time interval, from first use until user requirements are no longer met, due to economics of operation and maintenance, or obsolescence

Note 1 to entry: In this context, “first use” excludes testing activities prior to hand-over of the item to the end-user.

[SOURCE: IEC 60050-192:2015, 192-02-27]

3.2 Abbreviated terms

FIT	Failures in time
METBF	Mean (elapsed) time between failures
MTBF	Mean operating time between failures
MTTF	Mean operating time to failure
MTTR	Mean time to restoration
T_M	Mission time
FMEA	Fault modes and effects analysis
FTA	Fault tree analysis
RBD	Reliability block diagram
PoF	Physics of failure

4 System reliability

Typically, an automation system consists of several different types of sub-systems, automation devices and accessories, and requires consistency in the reliability data of the automation system as well as automation devices.

The reliability of the system needs to consider the reliability of hardware, including interface, communication, etc. In addition to hardware reliability, other factors such as software, human factor, security, may also be considered (see Annex A).

NOTE Communication in this document means the hardware used for communication, such as cable, router.

5 Calculation of system reliability

5.1 General

This document provides guidance for calculation of system reliability for simple system structures with constant failure rates for its elements, based on reliability block diagrams. For these and other type of system structures, e.g. k-out-of-n structures, see e.g. IEC 61078. For more information about other calculation methods for systems, see e.g. IEC 60300-3-1.

Reliability data from observation of devices in the field and laboratory test are not addressed in this document, but it is referred to IEC TS 63164-1.

Every single element of the system needs to have reliability data, like MTTF, MTBF, λ or B_{10}. To calculate the whole system all single elements need the same kind of data.

Some values for reliability data can be derived as following under certain conditions, see IEC 61703.

Example:

MTTF = $1/\lambda$ (for constant failure rate)

$\lambda = 0{,}1 \times C/B_{10}$ (assuming constant failure rate), where C is equal to the number of operations per hour and B_{10} is given in cycles, see IEC 62061.

In addition to random failure, systematic failure is also very common in automation systems. The calculation methods in the main part of this document focus on random failure, while avoiding or reducing systematic failure can also improve the reliability of the system (see Annex B).

5.2 Form to present reliability data

Generally, the reliability data can be considered from the following aspects. More details could be found in IEC TS 63164-1.

Reliability data: Common reliability data such as MTBF, MTTF or λ.

Reference conditions: Information about deployment conditions under which the system reliability was calculated, such as operating time, exposure time, operating voltage, operating current, duty cycle.

Reference environment conditions: Information about the reference environment conditions which are assumed to be the system environment, such as temperature, humidity, pressure, corrosion, vibration.

Events: Information about anything that happened to the automation system during its life and might influence reliability, such as maintenance information.

5.3 Structures and calculations

5.3.1 Basic formulas

In this subclause, some basic formulas related to reliability are given, which can also be found e.g. in IEC 61703.

For non-repairable items or systems, the commonly used reliability function $R(t) = R(0,t)$ with $R(0) = 1$ is given by the following formula

$$R(t) = \exp\left(-\int_0^t \lambda(u)\,du\right) \tag{1}$$

where $\lambda(u)$ is the instantaneous failure rate of the item. In other words, the reliability function expresses the probability of survival until time t. For a constant failure rate λ (i.e., exponentially distributed failure times), the above formula simplifies to

$$R(t) = e^{-\lambda t} \tag{2}$$

The mean operating time to failure (MTTF) in case of non-repairable items or systems, M_{TTF} can be calculated by the formula

$$M_{TTF} = \int_0^\infty R(t)\,dt \tag{3}$$

where, only in the case of exponentially distributed failure times, this reduces to

$$M_{TTF} = \frac{1}{\lambda} \tag{4}$$

While a value for the MTTF can be calculated for virtually any failure time distribution with corresponding constant or non-constant failure rate, for the converse calculation of a constant failure rate from the MTTF it should be ensured that the failure rate is indeed constant. In particular, this is not the case for a redundant system of non-repairable components, as the failure rate of the redundant system is not constant. Sometimes, however, an averaged constant failure rate can be calculated over a certain time period and used further with reasonable accuracy, in order to simplify the analysis.

For repairable items, the mean operating time between failures (MTBF, IEV 192-05-13) should be used instead of mean operating time to failure (MTTF, IEV 192-05-11). However, the two measures are essentially identical if the item is “as good as new” after restoration.

NOTE 1 For repairable items with negligible time to restoration, the mean operating time between failures (MTBF) is approximately equal to the mean (elapsed) time between failures (METBF, see 3.3 of IEC 61703:2016).

NOTE 2 For calculation of MTTF, the failure rate is assumed as 0 in the non-operating state.

5.3.2 Series structures

If each element of a system is required for the overall function of the system, the elements are to be considered in series, as shown in Figure 1.

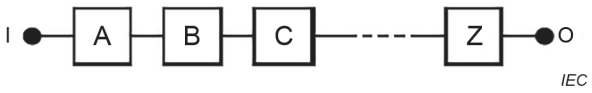

Figure 1 – Series reliability block diagram

For a series system the reliability function for the system is generally given by

$$R_s(t) = \prod_{i=A}^{Z} R_i(t) \tag{5}$$

If the individual elements have exponentially distributed failure times, then

$$R_i(t) = e^{-\lambda_i t} \tag{6}$$

and

$$R_s(t) = e^{-\lambda_s t} \tag{7}$$

$$\lambda_S = \lambda_A + \lambda_B + \lambda_C + \ldots. \lambda_Z \tag{8}$$

where

$R_s(t)$ represents the reliability function of the system;

$R_i(t)$ represents the reliability function of the different parts;

λ_S represents the constant failure rate of the system;

λ_i represents the constant failure rate of the different parts;

i ranges from A, B, C, …, to Z.

or

$$\frac{1}{M_{TBFSys}} = \frac{1}{M_{TBF,A}} + \frac{1}{M_{TBF,B}} + \frac{1}{M_{TBF,C}} + \cdots + \frac{1}{M_{TBF,Z}} \tag{9}$$

where

M_{TBFSys} represents the MTBF of the system;

$M_{TBF,i}$ represents the MTBF of the different parts.

NOTE 1 If the failure rate λ is expressed in FIT, the resulting of MTBF is expressed in hours.

NOTE 2 FIT is the failure rate expressed in number of failures that can be expected in one billion (10^9) device-hours of operation.

5.3.3 Parallel structures

If several elements of a system are required for the overall function of the system in a redundant manner, the elements are considered to be in parallel, as shown in Figure 2.

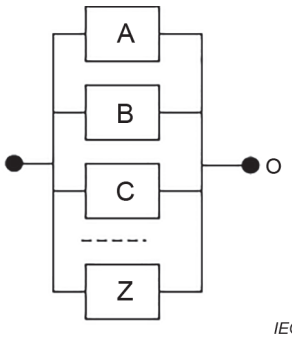

Figure 2 – Parallel reliability block diagram

For the system with non-repairable components, the following general formula is used:

$$R_s(t) = 1 - \prod_{i=A}^{Z}[1 - R_i(t)] \quad (10)$$

If the individual elements have exponentially distributed failure times, then

$$R_i(t) = e^{-\lambda_i t} \quad (11)$$

$$M_{TTFSys} = \int_0^\infty [1 - \prod_{i=A}^{Z}(1 - \mathrm{e}^{-\lambda_i t})]dt \quad (12)$$

where

$R_s(t)$ represents the reliability function of the system;

$R_i(t)$ represents the reliability function of the different parts;

M_{TTFSys} represents the MTTF of the system;

λ_i represents the constant failure rate of the different parts;

i ranges from A, B, C, … to Z.

NOTE 1 If the failure rate λ_i is expressed in FIT, the resulting of M_{TTFSys} is expressed in hours.

NOTE 2 For the above parallel system with non-repairable components, the failure rate of the system is not constant.

If the system can be considered as good as new after restoration, MTTF is equal to MTBF of the system.

For the system with repairable components, if the time to restoration is negligible compared to the mean operating time between failures, the following approximative formula is used:

$$M_{TBFSys} = \left(\prod_{i=A}^{Z}\frac{\lambda_i}{\mu_i}\sum_{i=A}^{Z}\mu_i\right)^{-1} \text{ for } \lambda_i \ll \mu_i \quad (13)$$

where

M_{TBFSys} represents the MTBF of the system;

λ_i represents the constant failure rate of the different parts;

μ_i represents the constant repair rate of the different parts, which is equal to the reciprocal of the MTTR for each part in case of exponentially distributed times to restoration;

i ranges from A, B, C, … to Z.

NOTE 3 If the failure rate λ_i and the repair rate μ_i are expressed in FIT, the resulting of M_{TBFSys} and $M_{TTR,i}$ are expressed in 10^9 hours.

5.3.4 Mixed structures

Frequently, a system cannot be modelled only with a simple series or parallel system. Then, it may be a mixed structure, as shown in Figure 3.

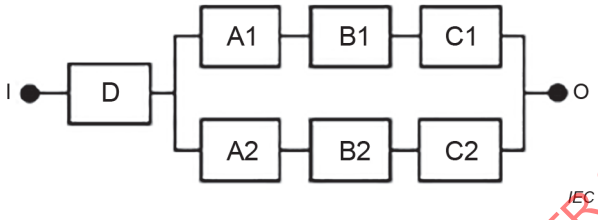

Figure 3 – General series-parallel (redundancy) reliability block diagram

The mixed structure may be reduced to serial and parallel structures, as shown in Figure 4.

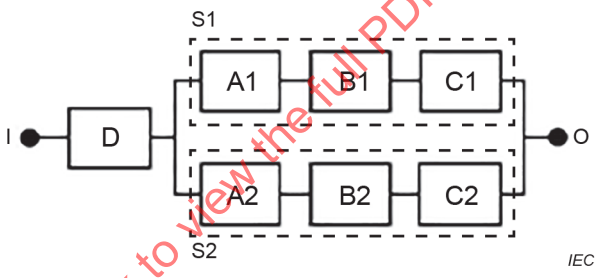

Figure 4 – Reduce the mixed structure

$$\lambda_{s1} = \lambda_{A1} + \lambda_{B1} + \lambda_{C1} \quad (14)$$

$$\lambda_{s2} = \lambda_{A2} + \lambda_{B2} + \lambda_{C2} \quad (15)$$

$$M_{TTFSys} = \int_0^\infty R_s(t)dt = \int_0^\infty e^{-\lambda_D t}\left[1 - \left(1 - e^{-\lambda_{S1} t}\right)\left(1 - e^{-\lambda_{S2} t}\right)\right]dt \quad (16)$$

where

λ_{s1} represents the failure rate of system S1, including A1, B1 and C1;

λ_{i1} represents the failure rate of device A1, B1 or C1 with *i* = A, B, C;

λ_{s2} represents the failure rate of system S2, including A2, B2 and C2;

λ_{i2} represents the failure rate of device A2, B2 or C2 with *i*=A, B, C;

λ_D represents the failure rate of device D;

$R_s(t)$ represents the reliability function of the system;

M_{TTFSys} represents the MTTF of the system.

NOTE If the failure rate λ is expressed in FIT, the resulting of M_{TTFSys} is expressed in hours.

5.3.5 Summary

Table 1 is a summary of common formulas related to system reliability.

Table 1 – Summary of common formulas related to system reliability

System reliability measure	Series structure	Parallel structure (hot standby)
Non-repairable items		
Survival probability $R_S(t)$	$\prod_i R_i(t)$	$1-\prod_i (1-R_i(t))$
Survival probability $R_S(t)$ (constant failure rates λ_i)	$\prod_i \exp(-\lambda_i\, t)$	$1-\prod_i (1-\exp(-\lambda_i\, t))$
Mean operating time to failure MTTF_S (constant failure rates λ_i)	$\left(\sum_i \lambda_i\right)^{-1}$	$\int_0^\infty R_S(t)dt$
Repairable items		
Mean operating time between failures MTBF_S (constant failure rates λ_i and repair rates μ_i)	$\left(\sum_i \lambda_i\right)^{-1}$	$\left(\prod_i \frac{\lambda_i}{\mu_i} \sum_i \mu_i\right)^{-1}$ for $\lambda_i \ll \mu_i$
Mean down time MDT_S (constant failure rates λ_i and repair rates μ_i)	$\sum_i \frac{\lambda_i}{\mu_i} (\sum_i \lambda_i)^{-1}$ for $\lambda_i \ll \mu_i$	$\left(\sum_i \mu_i\right)^{-1}$

Annex A
(informative)

Examples of typical automation systems

A.1 General

Automation system deals with the use of control systems and information technology to reduce manual work in the industrial production of goods and services. Automation systems are, for example, used for power generation, traffic management, water management, pulp and paper handling, printing, metal handling, oil refinery, chemical processes, pharmaceutical manufacturing, or carrier ships.

An example for series structure of simplified process automation system is given in Clause A.2, and an example for mixed structure of simplified process automation sub-system is given in Clause A.3.

A.2 Example for series structure of process automation system

A process automation or automation system (PAS) is used to automatically control a process such as metallurgy, chemical, oil refineries, paper and pulp factories, etc. The PAS often uses a network to interconnect sensors, controllers, operator terminals and actuators, as shown in Figure A.1.

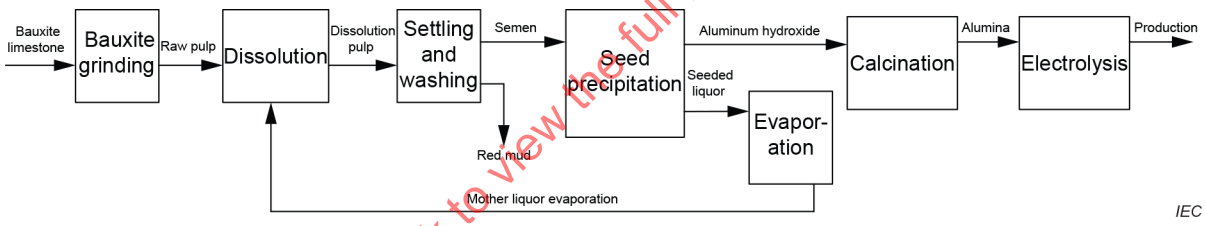

Figure A.1 – A typical process automation system (aluminum smelting)

Figure A.2 depicts the automation system configuration for aluminum smelting. The automation system configuration for aluminum smelting includes the following production processes:

a) bauxite grinding process (marked as A1);

b) dissolution process (marked as A2);

c) settling and washing process (marked as A3);

d) seed precipitation process (marked as A4);

e) evaporation process (marked as A5);

f) calcination process (marked as A6);

g) electrolysis process (marked as A7).

Figure A.1 can be depicted as a block diagram in Figure A.2.

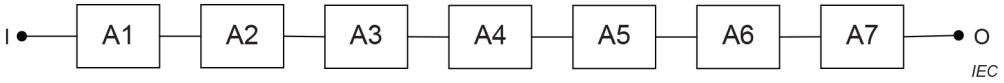

Figure A.2 – Block diagram for aluminum smelting automation system

The block diagram for the aluminum smelting system is a series structure. A1, A2, …, A7 denote the sub-system of the aluminum smelting automation system, and A1, A2, …, A7 are independent and required for the overall function of aluminum smelting system.

The MTBF values of the aluminum smelting automation system is denoted as $M_{TBF,Ai}$ (i=1, 2, … 7).

The system reliability λ of the aluminum smelting automation system is calculated by RBD as

$$\lambda_S = \lambda_{A1} + \lambda_{A2} + \lambda_{A3} + \lambda_{A4} + \lambda_{A5} + \lambda_{A6} + \lambda_{A7} \quad \text{(A.1)}$$

or

$$\frac{1}{M_{TBFSys}} = \frac{1}{M_{TBF,A1}} + \frac{1}{M_{TBF,A2}} + \frac{1}{M_{TBF,A3}} + \frac{1}{M_{TBF,A4}} + \frac{1}{M_{TBF,A5}} + \frac{1}{M_{TBF,A6}} + \frac{1}{M_{TBF,A7}} \quad \text{(A.2)}$$

where

λ_S represents the failure rate of the system;

λ_{Ai} represents the failure rate of different parts (A1 to A7);

M_{TBFSys} represents the MTBF of the system;

$M_{TBF,Ai}$ represents the MTBF of different parts (A1 to A7).

A.3 Example for mixed structure of process automation sub-system

Take settling and washing process of an aluminum smelting automation system as an example to calculate λ_{A3}. The settling and washing process is shown in Figure A.3.

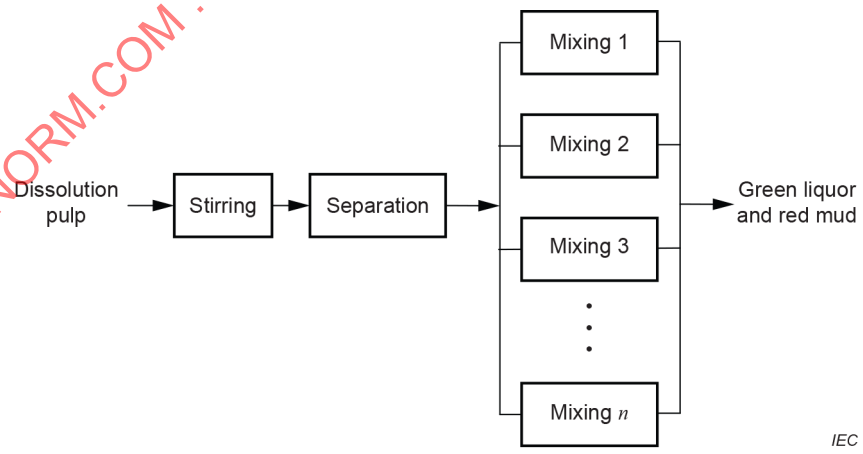

Figure A.3 – Settling and washing process for aluminum smelting automation system

Figure A.3 can be depicted as a block diagram in Figure A.4.

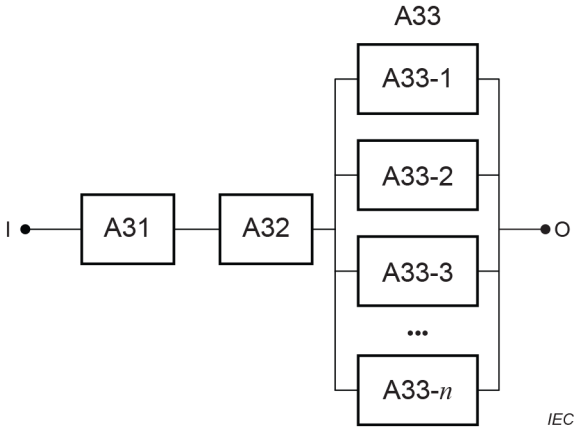

Figure A.4 – Block diagram for settling and washing process

The block diagram for the settling and washing process is a mixed structure. A31, A32, and A33 denote the sub-system of the settling and washing process, and A33-1, A33-2, …, A33-n are independent. A33-1, A33-2, …, and A33-n are required for the overall function of settling and washing process in a redundancy way. A33-1, A33-2, …, and A33-n are considered to be in parallel.

The sub-system MTBF values of the settling and washing process is denoted as $M_{TBF,A3i}$ (i=1, 2, 3).

The system reliability λ_{A3} of the settling and washing process is calculated by RBD as

$$R_{A33}(t) = 1 - \prod_{i=1}^{n}[1 - R_{A33-i}(t)] = 1 - \prod_{i=1}^{n}\left(1 - \mathrm{e}^{-\lambda_{A33-i}t}\right) \quad \text{(A.3)}$$

$$R_s(t) = R_{A31}(t) \cdot R_{A32}(t) \cdot R_{A33}(t) = e^{-(\lambda_{A31}+\lambda_{A32})t}\left[1 - \prod_{i=1}^{n}\left(1 - \mathrm{e}^{-\lambda_{A33-i}t}\right)\right] \quad \text{(A.4)}$$

$$M_{TBFSys} = \int_0^{\infty} R_s(t)dt = \int_0^{\infty} e^{-(\lambda_{A31}+\lambda_{A32})t}\left[1 - \prod_{i=1}^{n}\left(1 - \mathrm{e}^{-\lambda_{A33-i}t}\right)\right]dt \quad \text{(A.5)}$$

where

$R_{A33}(t)$ is the reliability of system A33;

$R_{A33-i}(t)$ is the reliability of devices in system A33 (i=1, 2, 3);

λ_{A33-i} is the failure rates of devices in system A33 (i=1, 2, 3);

$R_s(t)$ is the reliability of the system;

$R_{A31}(t)$ is the reliability of device A31;

$R_{A32}(t)$ is the reliability of device A32;

λ_{A31} is the failure rate of device A31;

λ_{A32} is the failure rate of device A32;

M_{TBFSys} is the MTBF of the system.

Annex B
(informative)

Methods to improve the system reliability

B.1 General

The failure of the automation system will lead to the decrease of reliability. The reliability of the automation system can be improved by reducing or avoiding the failure of the automation system.

The failure of the automation system can be divided into systematic failure and random hardware failure. This appendix provides general methods for reducing systematic failure and random hardware failure. Additional guidance for improving system reliability can be found in IEC 60300-3-15.

B.2 Methods to reduce systematic failure

B.2.1 General

Systematic failure is a man-made failure, which can be eliminated by changing the design, production process, operation mode and other factors. Systematic failures can be avoided and controlled through the following methods.

B.2.2 Measures to avoid systematic failure

The following measures for avoidance of systematic failures are implemented during the different phases of the lifecycle, where they can be applied either for hardware, for software, or for both.

a) design requirements specification phase: project management, documentation, structured specification, inspection of the specification, computer-aided specification tools, etc;

b) design and development phase: project management, documentation, observance of guidelines and standards, structured specification, inspection of the specification, computer-aided specification tools, semi-formal methods, formal methods, etc;

c) system integration phase: project management, documentation, functional testing, black-box testing, field experience, statistical testing;

d) operation and maintenance phase: project management, documentation, operation and maintenance instructions, protection against operator mistakes.

NOTE These measures can be implemented based on the V-model for the development process. For one example, how to use the V-model see software development in IEC 61508-3:2010. In addition, the information from operation or maintenance phase could be used for the development of future systems.

B.2.3 Measures to control systematic failure

The following methods are adopted to control systematic failure in design, including:

a) techniques and measures to control systematic failures caused by equipment: program sequence monitoring, failure detection by on-line monitoring, code protection, diverse hardware, stress screening, accelerated life testing and measures based on PoF;

NOTE 1 Equipment includes hardware, software, interface, network, etc. As for network dependability could refer to IEC 61784-3, IEC 62673 and IEC 61907.

NOTE 2 The physics of failure (PoF) approach can be used in reliability design and assessment, which is an attempt to identify the “weakest link” of a design to ensure that the required equipment life and reliability is exceeded by the design. Measures based on POF includes FEA modelling, failure mechanism modelling, failure probability density calculation and necessary testing, these measures are usually used to deal with solder joint failure. More details refer to IEC 61709:2017, Annex F.