IEC 61069-2

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment –
Part 2: Assessment methodology

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation –
Partie 2: Méthodologie à appliquer pour l'évaluation

IEC 61069-2:2016-06(en-fr)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 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 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: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61069-2

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

**Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment –
Part 2: Assessment methodology**

**Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation –
Partie 2: Méthodologie à appliquer pour l'évaluation**

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40 ISBN 978-2-8322-3410-5

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 2: Assessment methodology

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.

International Standard IEC 61069-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1993. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Reorganization of the material of IEC 61069-2:1993 to make the overall set of standards more organized and consistent;
b) IEC TS 62603-1:2014 has been incorporated into this edition.

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

FDIS	Report on voting
65A/790/FDIS	65A/799/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.

A list of all parts in the IEC 61069 series, published under the general title *Industrial-process measurement,control and automation – Evaluation of system properties for the purpose of system assessment*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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.

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

IEC 61069 deals with the method which should be used to assess system properties of a basic control system (BCS). IEC 61069 consists of the following parts:

Part 1: Terminology and basic concepts

Part 2: Assessment methodology

Part 3: Assessment of system functionality

Part 4: Assessment of system performance

Part 5: Assessment of system dependability

Part 6: Assessment of system operability

Part 7: Assessment of system safety

Part 8: Assessment of other system properties

Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the particular mission or class of missions.

Since this is rarely practical, the rationale on which an assessment of a system should be based is:

– the identification of the importance of each of the relevant system properties;

– the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations can still be specified and carried out for use in assessments performed by others. In such cases, the standard can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.

In preparing the assessment, it may be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, e.g., a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the “new” BCS; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns.

The part structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

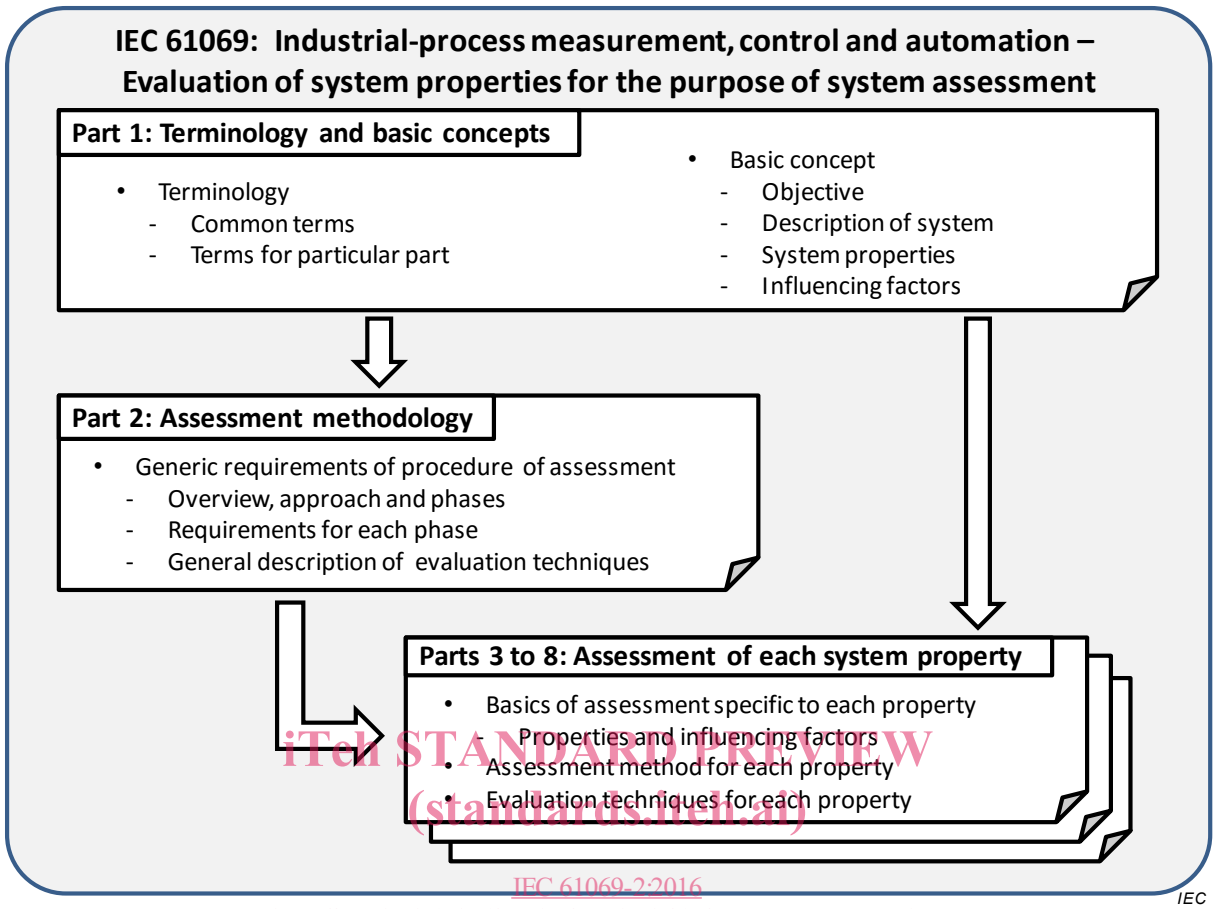

Figure 1 – General layout of IEC 61069

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 2: Assessment methodology

1 Scope

This part of IEC 61069 specifies the methodology in the assessment of a basic control system (BCS) based on the basic concepts of IEC 61069-1.

It describes the method for analysing, weighing the relative importance of the various system properties and influencing factors, and determining an assessment program.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61069-1:—[1], *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61069-1 apply.

3.2 Abbreviated terms, acronyms, conventions and symbols

For the purposes of this document, the abbreviated terms, acronyms, conventions and symbols given in IEC 61069-1 apply.

4 Assessment approach

BCSs are sufficiently complex, so that a totally comprehensive assessment inevitably requires an expenditure of effort and time that is neither practical nor cost-effective. It is therefore important to analyse and specify the objectives of the assessment carefully, before an assessment program is planned.

The mission of the system or class of missions is broken down into tasks.

The task(s) which the system needs to perform should be defined in terms of the selected BCS, its system properties, and the required functions. This enables the functions required for the system to fulfil its mission(s) to be specified precisely.

---

[1] Second edition to be published simultaneously with this part of IEC 61069.

Missions of the system usually require some characteristics of the system which are not directly related to the tasks of the system. Such characteristics include documentation and support services.

The assessment program shall be designed with the assessment objectives, the system requirements and the system specifications. It should be prepared in advance.

NOTE In certain cases, e.g. a regulated application, it may be necessary that the assessment be designed and performed by an independent party.

In the absence of a mission, no assessment can be made; however, examination of the system to gather and organize data for a later assessment is possible.

5 Assessment method

5.1 Overview

5.1.1 General

The details of the assessment program shall be derived from consideration of the assessment objectives (as stated in 5.2) and the following inputs:

– System Requirements Document (SRD), and
– System Specification Document (SSD).

NOTE 1 Systems Requirements Document is explained in Annex A.

NOTE 2 System Specification Document is explained in Annex B.

The assessment correlates items of the system requirements document with the system specification document guided by the assessment objective.

If at any phase of the assessment information from the SRD or SSD is missing or incomplete, the originators of the SRD or SSD should be consulted with specific questions to obtain the required further information.

The assessment method is a tool to be utilized during the life cycle of BCS. Yet the life cycle is out of scope of IEC 61069-2. Still during the development of a BCS and defining its assessment, the overall BCS life cycle should be taken into account.

Assessments for every relevant stages of the life cycle should be planned, e.g. commissioning.

5.1.2 Phases

The assessment consists of the following phases:

– Defining the objectives of the assessment;
– Design and layout of the assessment;
– Planning of the assessment program;
– Execution of the assessment;
– Reporting of the results.

The phases and their respective inputs and outputs are shown in Table 1.

Table 1 – Assessment phases, inputs and outputs

Phase	Input	Output
Defining the objectives of the assessment	SRD and SSD	(Documented) Objective of the assessment Assessment protocol
Design and layout of the assessment	Objective of the assessment SRD SSD	Assessment specification
Planning of the assessment program	Assessment specification	Assessment program
Execution of the assessment	Assessment program	Result of the evaluations
Reporting of the results	Result of the evaluations	Report of the assessment

5.2 Defining the objectives of the assessment

The objectives of the assessment shall be stated and documented prior to the start of the assessment as a foundation for planning and preparation of the assessment program. They should be stated clearly and carefully.

These objectives form the basis of the guiding principles throughout the assessment by:

- determining the scope,
- the nature of the evaluation,
- the depth of the evaluation to be carried out,
- the measurements and observations to be made,
- the type of reports to be produced.

The objectives govern the cost of the assessment and the resources required to conduct the assessment.

It is therefore of utmost importance that the objectives and the scope of the assessment are well-documented and agreed upon before the assessment program is further developed.

Description of the magnitude of BCS change requiring a reassessment should be defined, e.g. BCS expansion.

Updates of the assessment, during the BCS life cycle, regardless of changes/expansion, should be defined/scheduled, e.g. after 10 years of operation.

The authority(ies) who may require an assessment or re-assessment should be defined.

Additionally the authority(ies) who approve assessments or re-assessments should be defined.

During the assessment, reviews should be carried out at planned review points or at pre-determined intervals. Such reviews should at least be held at the end of each phase.

The objectives of the assessment may be, for example:

– to assess a specific system for a particular mission;
– to assess a variety of configurations of a single system for a particular mission;
– to compare several systems for a particular mission;
– to obtain an assessment of a particular system for general use in a variety of missions;

– to establish the suitability of a system for a particular mission;
– to establish the suitability of a system for a defined class of missions.

The assessment protocol shall be defined including:

– the assessment authorities for change and release of the assessment program,
– the assessment specifications and the assessment reports,
– the procedures to be followed,
– the contingency actions that are permissible without seeking prior authorization in the event that the assessment cannot be conducted as planned.

5.3 Design and layout of the assessment

5.3.1 Defining the scope of assessment

5.3.1.1 System boundary

The boundary of the system shall be carefully defined by identifying "what does and what does not" belong to the system to be assessed.

The boundary of the system to be assessed shall be defined by taking into account all aspects of influencing factors described in IEC 61069-1; — ,5.3 . It shall be documented in the assessment specification.

The system boundary can be physical (e.g. equipment, geography) and/or virtual (e.g. information, communication).

The objectives of the assessment are translated into a scope of the assessment. In order to develop the scope, the system properties described in IEC 61069-1; —, 5.2.2 to 5.2.7 shall be taken into consideration.

5.3.1.2 System configuration

The configuration(s) of the system to be assessed shall be specified in the assessment specification. Since the configurability of the system itself can be a system property to be assessed, the configuration of the system where the assessment items are evaluated should be carefully specified.

If the assessment objective is to assess a specific system for a particular mission, the assessment shall be carried out on a specific system configuration and this configuration shall be documented in the assessment specification.

If the assessment objective is to assess the flexibility of a system to meet a broad range of typical requirements encountered in a specific sector of industry, the assessment shall be carried out on a range of defined modules that can be configured in a variety of alternative ways. The range of modules and the variety of configurations shall be documented in the assessment specification.

A system is sometimes so complex that comprehensive evaluations of all system properties would not be cost-effective, or even feasible. By careful consideration of the objectives, the system configuration and the influencing factors, the evaluations can be reduced to include only those assessment items which are most sensitive for the mission of the system.

5.3.2 System properties and influencing factors

The assessment items required for the assessment shall be specified. The required value or range of value of each system property and influencing factor shall also be specified.

Additionally, as far as applicable, influencing factors as described in IEC 61069-1 should be included.

Each assessment item should be scrutinized to determine whether it influences or degrades the system in such a way that it hampers or prohibits the correct conduct of other assessment items.

These considerations shall be documented as an assessment specification to show the constraints upon the sequencing of the assessment activities.

A convenient way to document the system properties and the influencing factors is in the form of a matrix, where the cells correspond to the assessment items.

A generic matrix to summarize an assessment is given in Figure 2.

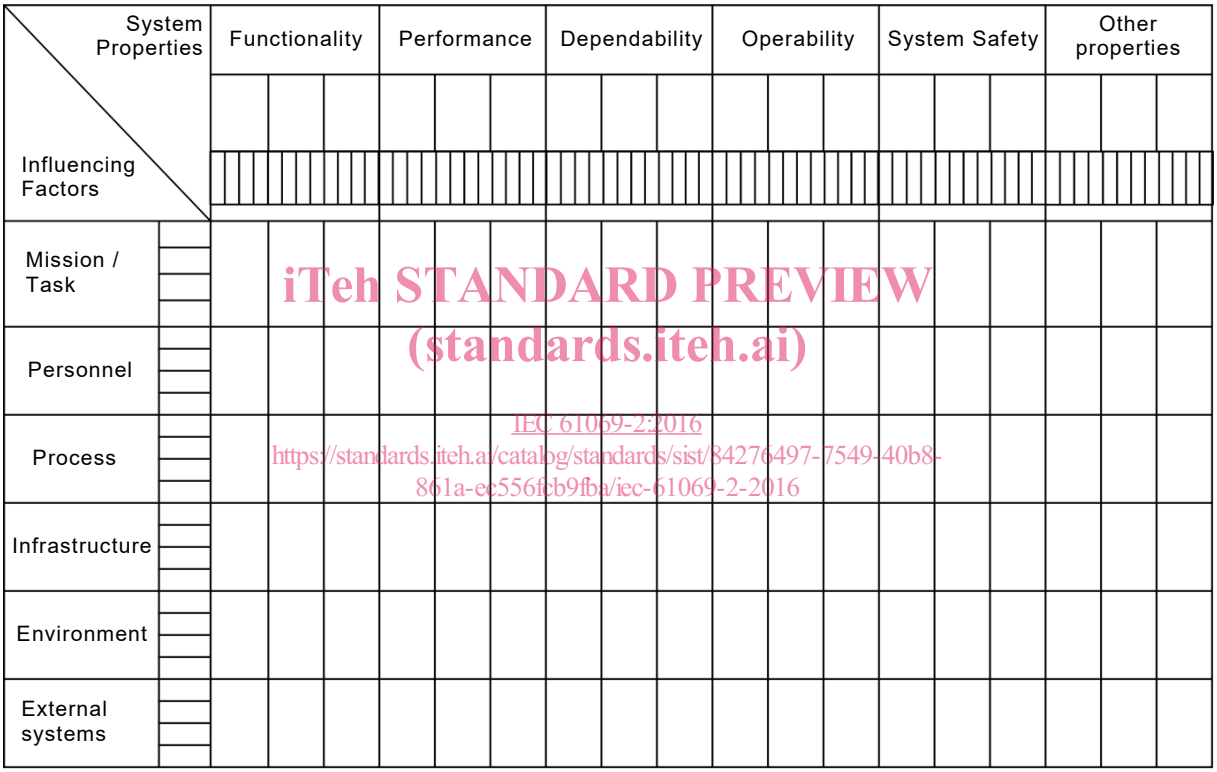

Figure 2 – Assessment matrix

The assessment items required to be included in the assessment shall be selected and their relative priorities shall be determined. It can be done using this matrix as a means for considering each system property and each influencing factor and taking into consideration the objective of the assessment.

An assessment item can be progressively further detailed by using e.g. groups or sub-groups of properties, in which the headings of the generic matrix are further expanded into more detailed system properties and influencing factors.

Assessment items, not relevant for the particular assessment, should also be identified for later reference, and the reasons for the exclusion should be documented.

5.3.3 Collation of documented information

The collation is a step of this phase to extract the information which is required to determine potential candidates of the assessment items. The information provided by this process is used for design and layout of the assessment.

For the purpose of the collation, the necessary information shall be extracted from the SRD and the SSD.

The SRD and SSD shall be carefully scrutinized to compile precise and concise statements of the topics. Example topics include:

– the boundaries of the system,
– the areas of non-compliance between system requirements and system specification,
– the list of required and future tasks,
– the list of functions provided to perform each of the required and future tasks,
– the list of alternative data paths linking the functions to support the required task(s),
– the allocation of the functions to the modules and elements,
– the number of these modules and elements,
– the extent to which these modules and elements are used to fulfil the required tasks,
– the system properties for each of the above functions,
– the influencing factors for each of the above modules/elements.

A list of potential assessment items shall be created from these topics. The assessment items shall be specified under specific system configuration(s) according to the objective of the assessment.

Each potential assessment item shall be examined to decide the extent to which this item is evaluated to obtain the required increase in the level of confidence.

The statements should be described in qualitative and quantitative terms, and, if applicable, their range of values.

NOTE Examples of collation documentation are provided in Annex C.

Each task to be assessed should be described in terms of its inputs, outputs and operation.

For each input, notes should be made of:

– permissible input states and corresponding permissible output state(s);
– non-permissible input states and corresponding action(s) required.

For each output, notes should be made of:

– permissible output states;
– non-permissible output states and corresponding action(s) required.

For each of the tasks, the following information about tasks should be clearly stated:

– kinds of failures which affect each task;
– permissible frequency of occurrence of each failure;
– action to be taken for each failure;
– maximum time during which the task can be stopped before the module is restored.