

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Intelligent device management –
Part 2: Requirements and recommendations**

**Gestion des appareils intelligents –
Partie 2: Exigences normatives et recommandations**

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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 une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Intelligent device management –
Part 2: Requirements and recommendations**

**Gestion des appareils intelligents –
Partie 2: Exigences normatives et recommandations**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-9485-7

**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

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, abbreviated terms and conventions	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	12
3.3 Conventions.....	13
4 Foundational requirements for IDM.....	13
4.1 Objective	13
4.2 General.....	13
4.3 Management functions.....	14
4.4 Formal and informal work processes and procedures.....	14
4.5 Management of change.....	15
4.5.1 General	15
4.5.2 Impact assessment.....	15
4.5.3 Planning	15
4.5.4 Training.....	16
4.5.5 Documentation	16
4.5.6 Retention of data and documents	16
4.6 Risk management	16
5 Risk management.....	16
5.1 Objective	16
5.2 General.....	16
5.3 IDM program requirements.....	17
5.4 Program coordination.....	17
5.5 Facility level risk management	17
5.6 Supplier risk management.....	19
5.7 Information management risks	19
5.8 Cybersecurity risk management	19
6 Enterprise level management for IDM.....	19
6.1 Objective	19
6.2 General.....	20
6.3 Organization and resources	20
6.4 Developing and maintaining IDM program	21
6.5 Supplier management	22
6.5.1 Co-ordination with suppliers	22
6.5.2 Intelligent device life cycle management.....	22
6.5.3 Device technology life cycle.....	23
6.6 Developing and maintaining IDM work process templates	23
6.7 IDM program management and design.....	24
6.7.1 Resource management.....	24
6.7.2 IDM program design and performance improvement	24
6.7.3 IDM program performance feedback to management	25
6.7.4 IDM program operation	25
6.7.5 IDM program support and monitoring for facilities	25

7	Implementing coordination between enterprise, facilities, and suppliers	25
7.1	Objective	25
7.2	General	26
7.3	Implementing IDM	26
7.3.1	Common principles	26
7.3.2	Implementing IDM in new facilities	26
7.3.3	Implementing IDM in existing facilities	27
7.3.4	Implementing IDM work processes in a facility	27
7.4	Coordination for continuous improvement	28
7.4.1	General	28
7.4.2	Assessment and audits of IDM activities	28
7.4.3	Resolving causes of program non-compliances	28
7.5	Coordination with other enterprise programs	29
7.5.1	General	29
7.5.2	Life cycle coordination of program activities	29
7.5.3	Applications	29
7.5.4	Device/process information	29
7.5.5	Systems, networks, and security	29
7.5.6	Life cycle phases	30
7.5.7	Application interfaces for coordination	30
8	Facility life cycle phases	30
8.1	Objective	30
8.2	General	30
8.3	Managing facility life cycle phases	31
8.3.1	General	31
8.3.2	Life cycle entry points	31
8.3.3	Facility modifications	31
8.4	Scope development	32
8.4.1	General	32
8.4.2	Objective	33
8.4.3	Risk management	33
8.4.4	Project type considerations	34
8.4.5	Planning and design of the IDM implementation	34
8.4.6	Defining facility long term support plans	35
8.4.7	Handover plan to operations and maintenance	35
8.4.8	Defining strategy for intelligent device cybersecurity	36
8.4.9	Selecting design alternatives	37
8.4.10	Preparing tools and their procedures	38
8.4.11	Selecting suppliers	39
8.4.12	Information management planning	40
8.5	Design and engineering	40
8.5.1	Objective	40
8.5.2	General	40
8.5.3	Device selection	42
8.5.4	Procurement of intelligent device	43
8.5.5	Configuration data preparation	44
8.5.6	Implementing and integrating intelligent device functions with IACS	49
8.5.7	System integration and testing requirements	51
8.6	Construction and commissioning	51

8.6.1	General	51
8.6.2	Site staging	52
8.6.3	Installation	53
8.6.4	Provisioning	53
8.6.5	Configuration	53
8.6.6	Loop-checking and commissioning	54
8.6.7	Training and personnel competency	55
8.6.8	Handover	56
8.6.9	PSSR	56
8.6.10	Startup	56
8.7	Operations and maintenance	56
8.7.1	General	56
8.7.2	Intelligent device continuous monitoring, problem identification, problem diagnosis processes	57
8.7.3	Intelligent device calibration	58
8.7.4	Repair processes	59
8.7.5	Intelligent device replacement	61
8.7.6	Intelligent device inventory management	64
8.7.7	Post-repair processes	65
8.8	Turnarounds	66
8.8.1	General	66
8.8.2	Preparation for turnaround	67
8.8.3	Turnaround planning	67
8.8.4	Turnaround execution	67
8.8.5	Recommission and start-up	68
8.9	Decommissioning	68
8.9.1	General	68
8.9.2	Archiving IDM data	68
8.9.3	Removal of devices	68
8.9.4	Refurbishment (for return to inventory)	69
8.9.5	Disposal (non-salvage)	69
9	Supplier requirements	69
9.1	Objective	69
9.2	General	69
9.3	Products	69
9.3.1	Devices	69
9.3.2	IACS	70
9.3.3	Software	71
9.4	Services	72
9.4.1	Engineering/project support	72
9.4.2	Operations and maintenance support	72
9.4.3	Personnel competency	72
9.4.4	Cybersecurity	73
9.5	Device support tools	73
9.5.1	Intelligent device templates	73
9.5.2	IDM toolkits	73
9.5.3	Interoperability support of intelligent device management system	74
9.5.4	Migration, configuration, and maintenance tools	74
10	Information management	74

10.1	Objective	74
10.2	General.....	75
10.3	Information collection, exchange, reconciliation, and storage	75
10.3.1	Collection and reconciliation	75
10.3.2	Cybersecurity	76
10.3.3	Information storage and retention procedures	76
10.3.4	Data management functions	77
10.4	IDM information	78
10.4.1	General	78
10.4.2	Information: Maintenance and reliability records	78
10.4.3	Information: Models and calculations	79
10.4.4	Information: Documents and drawings	79
10.4.5	Information: Identification of work processes and procedures	79
10.4.6	Information: Worker role competency.....	79
10.4.7	Information: Intelligent device configuration	79
10.4.8	Information: Toolkits	80
Annex A (informative)	Clause explanation notes	81
A.4	Foundational requirements for IDM	81
A.4.1	Objective	81
A.4.2	General	81
A.4.3	Management functions.....	81
A.4.4	Formal and informal work process and procedures	81
A.4.5	Management of change	81
A.5	Risk management	81
A.5.1	Objective	81
A.5.2	General	81
A.5.3	IDM program requirements	82
A.5.4	Program coordination	82
A.5.5	Facility level risk management.....	82
A.5.6	Supplier risk management	82
A.5.7	Information management risks	82
A.5.8	Cybersecurity risk management.....	82
A.6	Enterprise level management for IDM	82
A.6.1	Objective	82
A.6.2	General	82
A.6.3	Organization and resources	83
A.6.4	Developing and maintaining IDM program.....	83
A.6.5	Supplier management.....	84
A.6.6	Developing and maintaining IDM work process templates	84
A.6.7	IDM program management and design.....	85
A.7	Implementing coordination between enterprise, facilities, and suppliers	85
A.7.1	Objective	85
A.7.2	General	85
A.7.3	Implementing IDM.....	85
A.7.4	Coordination for continuous improvement.....	86
A.7.5	Coordination with other enterprise programs.....	86
A.8	Facility life cycle phases	87
A.8.1	Objective	87
A.8.2	General	87

A.8.3	Managing facility life cycle phases	87
A.8.4	Scope development	88
A.8.5	Design and engineering	90
A.8.6	Construction and commissioning	91
A.8.7	Operations and maintenance	93
A.8.8	Turnarounds	96
A.8.9	Decommissioning	97
A.9	Supplier requirements	97
A.9.1	Objective	97
A.9.2	General	97
A.9.3	Products	97
A.9.4	Services	98
A.9.5	Device support tools	98
A.10	Information management	98
A.10.1	Objective	98
A.10.2	General	98
A.10.3	Information collection, exchange, reconciliation, and storage	98
A.10.4	IDM information	99
Bibliography		100
Figure A.1	– Overview of loop repair process	94
Figure A.2	– Overview of new design evaluation and intelligent device replacement	95
Table A.1	– Installation guideline documents	92

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INTELLIGENT DEVICE MANAGEMENT –

Part 2: Requirements and recommendations

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63082-2 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC Technical Committee 65: Industrial-process measurement, control and automation. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65E/1079/FDIS	65E/1112/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 63082 series, published under the general title *Intelligent device management*, 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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

INTRODUCTION

The purpose of the IEC 63082 series is to define an environment that enables the effective use of intelligent devices. The IEC 63082 series defines common concepts, terminology, and management activities.

Intelligent device management (IDM) represents activities for managing intelligent devices through the facility life cycle and does not imply a particular asset management tool or set of those tools. Hardware and software tools are necessary to support work processes and procedures, but specification of the tools is not a part of the IEC 63082 series. IDM is one of many enterprise programs. IDM activities optimize the value from intelligent devices and supports integration of data from the production level with business systems. IDM is consistent with smart manufacturing initiatives.

Several stakeholders are responsible for delivering successful intelligent device management, including engineering, procurement, and construction (EPC) business providers, system integrators, suppliers and consultants.

The IEC 63082 series is not intended to replace or contradict other standards, for example IEC 61511 series for safety instrumented systems and IEC 62443 series for cybersecurity.

IEC TR 63082-1 defines intelligent device management concepts and terminology necessary for in-depth understanding and effective communication. It gives the basic concepts of how intelligent devices can be managed and an overview of how this device management works throughout the facility life cycle. IEC TR 63082-1 provides basic knowledge to understand the concepts of intelligent device management necessary to implement an IDM program.

This document provides provisions (requirements and recommendations). Additional information on why a requirement is given are provided in informative Annex A. The information provided in IEC TR 63082-1 is intended to be useful as background material for better understanding of provisions in this document.

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

INTELLIGENT DEVICE MANAGEMENT –

Part 2: Requirements and recommendations

1 Scope

This part of IEC 63082 specifies requirements and recommendations for establishing and maintaining intelligent device management (IDM) as outlined in IEC TR 63082-1 in an enterprise having one or more facilities.

The following topics are included in the scope of this document:

- optimizing functionality and performance of intelligent devices for their use;
- managing information related to IDM;
- integrating intelligent devices into industrial automation and control systems (IACS) in facilities;
- exchanging information between stakeholders that achieve and sustain IDM;
- coordinating multiple asynchronous IDM life cycles.

The following topics are outside the scope of this document:

- defining and determining the function and performance of intelligent devices;
- defining and specifying technologies and tools that provide, preserve and manage information related to IDM such as FDT, FDI, portable online and offline tools, configuration tools, historians, and maintenance planning tools;
- defining and specifying technologies and tools that are used to design intelligent devices;
- defining and specifying communication network architecture, communication technologies, cybersecurity requirements, and network management requirements.

2 Normative references

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

IEC 62381, *Automation systems in the process industry – Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)*

IEC 62382, *Control systems in the process industry – Electrical and instrumentation loop check*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC TR 63082-1:2020, *Intelligent device management – Part 1: Concepts and terminology*

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TR 63082-1 and the following apply.

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

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

3.1.1 certification

procedure by which a third party gives documented assurance that a product, process, or service conforms to specified requirements

[SOURCE: IEC 61400-22:2010, 3.4, modified – "written" was replaced with "documented" and "also known as conformity assessment" was deleted.]

3.1.2 decommissioning

act of taking an engineered system or component out of service, render it inoperative, dismantle and decontaminate it

[SOURCE: ISO 27914:2017, 3.13, modified – "decommission" was replaced with "decommissioning", and "take" was replaced with "act of taking".]

3.1.3 device monitoring

functions and activities to track behaviour of a device, and for all calls associated with the device

[SOURCE: ISO/IEC TR 18053:2000, 3.141, modified – "Device-Type Monitor" was replaced with "device monitoring", "A monitor that tracks" was replaced with "functions and activities to track", and "providing notification of events for the device" was removed.]

3.1.4 foundational requirement

requirement that serves as a basis for derivation of detailed requirements

EXAMPLE Management of risk, management of functionality and performance, management of change.

Note 1 to entry: It is possible that foundational requirements are not directly actionable, but their derived requirements should be a basis for action.

3.1.5 organization

body that is based on the membership of other bodies or individuals and has an established constitution and its own administration

[SOURCE: ISO/IEC Guide 2:2004, 4.2]

3.1.6 owner operator

enterprise or agency responsible for the day-to-day operation of a facility

Note 1 to entry: The owner operator can contractually delegate some or all these responsibilities.

3.1.7 quality management system QMS

organization framework whose structure provides the policies, processes, procedures, and resources required to implement the quality management plan

Note 1 to entry: The typical project quality management plan should be compatible to the organization's quality management system.

[SOURCE: ISO/IEC 30105-4:2016, 3.41, modified – "the" was deleted.]

3.1.8 requirement

expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed

Note 1 to entry: Requirements can describe an essential service, capability, feature or activity.

[SOURCE: ISO/IEC Directives Part 2:2021, 3.3.3]

3.1.9 supplier

party that produces, provides, or furnishes an item, system, or service

[SOURCE: ISO 28219:2017, 3.11, modified – "system" was added.]

3.1.10 tool

executable software program which interacts with the user to perform some function

EXAMPLE Link scheduling software (LSS).

[SOURCE: IEC 61158-4-2:2023, 3.4.73]

3.2 Abbreviated terms

AVL	approved vendor list
CAE	computer aided engineering
CMMS	computerized maintenance management system
DIN	Deutsches Institut für Normung (German Institute for Standardization)
DTM	device type manager
EAM	enterprise asset maintenance
EDD	electronic device description file
EPC	engineering, procurement, and construction
ERP	enterprise resource planning
FAT	factory acceptance test
FDI	field device integration
FDT	field device tool
HAZOP	hazard and operability study
HMI	human machine interface
IACS	industrial automation control system
IDM	intelligent device management
IED	intelligent electronic device

ISA	International Society of Automation
KPI	key performance indicator
LOPA	layer of protection analysis
MES	manufacturing execution system
MOC	management of change
MRO	maintenance repair and operations
MTBF	mean time between failures
NAMUR	Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie
NEC	national electrical code
NIST	National Institute of Standards and Technology
OT	operations technology
PAM	plant asset management
PSSR	pre-start-up safety review
PV	process variable
QMS	quality management system
RAM	responsibility assignment matrix
RFP	request for proposal
SAT	site acceptance test
SIT	site integration test

3.3 Conventions

To aid the user of this document with its understanding without requiring reference to IEC 63082-1, Annex A contains contextual information for each of the level 1 through 3 headings of the main document.

4 Foundational requirements for IDM

4.1 Objective

This clause specifies foundational requirements and recommendations for achieving and sustaining IDM.

Foundational requirements provide the basis for detailed or derived requirements in the balance of this document.

The requirements and recommendations in this clause apply to all activities, products and services related to IDM, and its management.

NOTE The products and the associated technologies include but are not limited to intelligent devices and IACS hardware and software. These foundational requirements apply to all life cycles.

4.2 General

IDM shall be established both for new and existing facilities.

All organizations involved in supply and distribution of intelligent devices, organizations that supply tools and services in support of intelligent devices, and organizations that use or operate facilities using intelligent devices shall be considered participants of the IDM program.

IDM shall be maintained and continuously improved for adapting to technology and organizational changes.

IDM should be implemented in a consistent manner across an enterprise with multiple facilities.

NOTE IDM assumes flexibility in how it is implemented to fulfil the needs of different facilities within an enterprise.

IDM shall cover integration of devices into the IACS.

4.3 Management functions

IDM shall include functions and organizations necessary for coordinating other management programs and internal and external organizational resources. Organizations shall ensure resources for IDM implementation are available.

NOTE 1 A primary goal of an IDM program is coordination with other external programs. For example: supplier alliance programs can provide input to and direct support for IDM.

NOTE 2 A program is an efficient and formal way to manage and coordinate activities such as IDM.

IDM shall provide support for risk management programs by providing data for evaluating related risks including those of hardware random failures, common cause failures (e.g., systematic, design, installation, integration, and maintenance), and cybersecurity.

IDM shall be developed with management sponsorship, ownership and accountability.

Procedures and processes shall be established to monitor and measure performance of IDM.

NOTE 3 KPIs are a commonly used technique to monitor and measure performance.

4.4 Formal and informal work processes and procedures

Organization having an IDM program shall decide if each of their work processes is a formal work process or an informal work process. Each IDM participating organization shall define the requirements of those work processes and procedures.

Work processes, procedures, and tasks necessary to achieve the foundational requirements shall be defined:

- the activities to be performed;
- the prerequisite skills and knowledge; and
- a training program to enable workers to develop these skills and knowledge.

Work processes include the subjects of:

- requirements for formal and informal work processes and procedures;
- requirement for a managed process for decisions, factors; and
- characteristics that determine informal versus formal work processes.

NOTE 1 Formal and informal work processes are derived from the foundational requirements.

NOTE 2 Formal work processes include processes where deviations from work processes and their associated deliverables are managed in accordance with the MOC requirements defined in the IDM program.

NOTE 3 Informal work processes include those accepted as being part of the basic training for a skilled work and encompass common good practices such as housekeeping.

The decision of making a work process formal or informal should be made based on but is not limited to the following criteria:

- a) high complexity;
- b) number of people or organizations involved;
- c) transitions in ownership or multiple owners;

- d) high risk levels;
- e) frequency of use;
- f) need for stability, reproducibility, and accuracy over long time periods.

Formal work processes and procedures should include but are not limited to:

- a) defined starting conditions or inputs;
- b) defined internal processes including defined roles and responsibilities;
- c) defined toolkits and infrastructure;
- d) defined staff resources (numbers, identity, and competency);
- e) defined external interfaces;
- f) defined completion and output;
- g) defined financial support, measures of success, and management accountability;
- h) formal documentation and training.

The IDM program shall address intelligent device security and cybersecurity requirements for the IACS.

NOTE 4 Intelligent device security is a condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

EXAMPLE IEC 62443 series specifies cybersecurity requirements for IACS.

4.5 Management of change

4.5.1 General

A management of change (MOC) shall be applied to all devices, systems, tools, work processes, information, and resources necessary to IDM.

NOTE 1 IDM changes include, but are not limited to, changes introduced by intelligent device suppliers, such as revision or technology changes; changes to IDM program; tools or procedures; and changes to personnel with IDM responsibility.

NOTE 2 MOC includes configuration management as described in 8.6.5.

IDM shall provide for MOC at all levels or sub levels of the enterprise's organization.

Personnel roles and responsibilities shall be defined in the IDM program for managing, executing, maintaining, and documenting changes to intelligent devices and intelligent device related IACS.

4.5.2 Impact assessment

Any modification activity shall not begin until an impact assessment is completed and approved in accordance with IDM procedures.

The impact assessment shall consider the short and long-term impact of the proposed modification. If the impact assessment shows that the proposed modification would negatively impact functional requirements, this impact shall be resolved before implementation.

NOTE Since intelligent device configurations are easy to change, it is important that only modifications that have successfully completed the impact assessment and MOC process are implemented.

4.5.3 Planning

Planning for the modification and subsequent re-verification shall be documented and distributed to all participants, including re-estimate of impact of change.

NOTE Change planning can vary with the change complexity and impact.

Modifications and re-verifications shall be carried out in accordance with the approved change plan.

4.5.4 Training

Affected personnel shall be trained in the practices related to intelligent device changes before the changes are implemented.

4.5.5 Documentation

All documentation affected by the change (including test and acceptance procedures) shall be updated as required by the IDM program.

4.5.6 Retention of data and documents

The specified system functionality shall be retained or achieved when changes are made that impact any intelligent device or connected components of IACS.

Historical records of changes shall be retained as defined by the IDM program.

Backups of intelligent device configurations and intelligent device connected IACS information shall be retained as specified by the IDM program.

4.6 Risk management

Risk related to IDM shall be included in the overall enterprise risk management strategy.

IDM risk management process shall be a formally defined systematic process.

5 Risk management

5.1 Objective

The IDM risk management process includes the identification of any potential threats that can occur during implementation of any IDM phase. This clause will identify complementary work processes an enterprise requires to eliminate, minimize or control any potential risks associated with IDM.

All provisions provided in this document should be satisfied to avoid unmanaged risk.

This clause will list risk management provisions throughout this document unique to IDM across the full life cycle.

5.2 General

IDM risk management shall identify the overall process to implement requirements for IDM, as defined by the enterprise.

Work processes for intelligent device criticality ranking should be integrated with existing enterprise risk management practices as documented in the IDM program.

IDM shall have mechanisms for mitigating risks associated with systematic and random failures, common cause failures, cybersecurity threats, financial impacts, and other identified risks.

5.3 IDM program requirements

The IDM program shall have work processes and management systems defined to monitor its effectiveness on a continuous basis.

IDM programs shall identify accountability for risk management results.

The IDM program shall define proactive measures to maintain program integrity.

NOTE 1 Proactive measures can include staffing, budget, tools, training and other activities associated with managing systematic risks.

Enterprise risk management provides alignment of strategies and processes to manage competing objectives and priorities associated with long term activities of the enterprise.

NOTE 2 Competing objectives and priorities can include capital expenditures, resource planning, maintenance activities, production schedule and other related activities.

IDM risk management shall identify and evaluate potential risks to all components, systems, work processes and tools.

NOTE 3 Each enterprise will determine the evaluation process to be used.

NOTE 4 The potential risks can include risk to the facility, suppliers and integrity of supply, enterprise goals and objectives and other factors.

5.4 Program coordination

IDM risk management shall be coordinated with other risk management programs at an enterprise and at a facility level.

NOTE 1 IDM risk management is not independent of enterprise and facility risk management programs.

NOTE 2 Program coordination is a core risk management activity.

NOTE 3 Risk assessment is a component of overall enterprise risk management; defining the requirements for the risk assessment is out of the scope of IDM.

IDM shall align with all work process requirements of the enterprise risk management strategy.

The IDM risk management process shall provide for implementation of internal and external risk management strategies.

NOTE 4 The internal and external risk management processes help to reduce the severity and/or likelihood of a risk.

NOTE 5 Internal and external risk management strategies can include coordination between production and maintenance, transportation systems, suppliers, unplanned events and other considerations.

The enterprise risk management process shall utilize the enterprise's risk management infrastructure to manage risks associated with IDM activities.

NOTE 6 The enterprise risk management process can be Layer of Protection Analysis (LOPA), Hazard and Operability Study (HAZOP), German Institute for Standardization (DIN: Deutsches Institut für Normung) matrix, Qualitative risk management (QRA), Fault tree analysis, and other defined programs.

5.5 Facility level risk management

Risk management shall be started at the beginning of the facility life cycle and continued throughout the full life cycle.

NOTE 1 The identification and management of risk early in the facility life cycle improves the effectiveness and efficiency of managing risk throughout the rest of the facility life cycle.

The IDM program shall ensure an evaluation of all risk triggers identified during the risk analysis process associated with IDM is completed.

Facilities shall use a life cycle management system fitted to their unique requirements that provides organization of a large number of sequential and parallel interdependent activities in order to manage risks associated with these activities.

NOTE 2 The generic life cycle model in 7.5 provides an example of the work processes and procedures for sequential and parallel facility risk management activities.

NOTE 3 The sequential and parallel activities can be defined in flowcharts, graphs, tables and other representations.

IDM program shall provide management for initial event triggers (such as random hardware failures), prior conditions, cascading effects and systematic contributions (such as procedures, lack of resources or inadequate training).

The IDM life cycle management system shall incorporate risk management measures to handle discontinuities between life cycle phases.

NOTE 4 Different life cycle phases include changes of personnel, roles and responsibilities, tools and the primary focus of activities. Transitions can be disruptive if not properly managed.

Changes late in a life cycle including out of sequence activities shall be managed through proper MOC and recycled through all appropriate life cycle activities.

NOTE 5 Out of sequence activities (such as rework) break dependencies that affect previously completed work.

NOTE 6 Determination of proper life cycle entry points ensures completion of necessary recycle activities (see 8.3).

Each life cycle phase shall have monitoring and auditing mechanisms to ensure that risks are managed.

Standard documentation shall be developed for all IDM program components.

NOTE 7 The standard documentation can include the use of templates and tools (see Clause 10 for information management).

Management of the life cycle risks shall include, as a minimum, risks associated with the following:

- a) Configuration data for each intelligent device and its host systems
 - 1) use of standard intelligent device templates and toolkits,
 - 2) parameters to be monitored and controlled,
 - 3) timely response and/or execution of corrective actions for
 - i) diagnostic conditions,
 - ii) failures,
 - iii) degraded or abnormal performance,
 - iv) security and access issues,
 - v) non-conformance to standards, regulations or requirements;
- b) Operations and maintenance strategy and planning
 - 1) workforce requirements,
 - 2) schedule,
 - 3) qualifications and training,
 - 4) quantity of skilled workers,
 - 5) frequency of testing and inspection;

c) Spare parts strategy

- 1) quantities,
- 2) locations.

5.6 Supplier risk management

The owner operator shall require suppliers to manage risks associated with products and services life cycles.

NOTE 1 Risks include but are not limited to product obsolescence and upgrades, changes associated with firmware and software revisions (refer Clause 9 for supplier requirements).

The owner operator shall require suppliers coordinate product and service risk management with enterprise programs and with facilities.

NOTE 2 Both suppliers and facilities work together to manage change (refer to 4.5).

5.7 Information management risks

Information management shall manage the risks associated with incomplete information sets.

Information management shall manage the risks associated with errors and discrepancies in information from diverse sources.

NOTE 1 Examples of diverse sources can include internal documentation, external documentation and other source data such as manuals, technical catalogues.

Information management shall manage risks associated with changes in information management systems, tools, personnel and procedures.

NOTE 2 An example of information changes in projects includes changes between the design and as-built.

NOTE 3 Examples are changes in personnel during handover from project team to a facility and changes in personnel at shift change (see 10.4).

5.8 Cybersecurity risk management

Consistent with cybersecurity principles, IACS access shall be associated with roles to the system and devices well defined and managed to minimum functionality to complete the tasks required.

IDM data integrity shall be maintained.

Isolation between different IACS elements, including IDM, shall be consistent with the IEC 62443 series zone and conduit system/defence-in-depth requirements.

Secure access and management of devices shall be part of the facility cybersecurity implementation practices.

6 Enterprise level management for IDM

6.1 Objective

This clause specifies requirements and recommendations for the development, maintenance, and improvement of enterprise level management for IDM.

Enterprise level IDM management includes but is not limited to:

- a) an IDM program including all management activities;
- b) infrastructure including host systems;
- c) resources including skills and budget;
- d) planning for and coordination of multiple life cycles including the IDM program life cycle, device technology life cycles, device life cycles, facility life cycles;
- e) coordination between facilities;
- f) work process templates.

NOTE Templates define elements of each IDM work process for a specific purpose common to many facilities of the enterprise. They are used as a basis for implementing IDM work processes in a specific facility.

6.2 General

The IDM program should apply to all facilities of the enterprise.

NOTE 1 Not all facilities have intelligent devices and therefore do not require IDM.

NOTE 2 IDM implementation can be phased in across multiple facilities.

IDM goals and objectives shall be fully documented in the IDM program.

The IDM program shall be communicated to responsible individuals and organizations with one or more IDM roles.

NOTE 3 IDM capability can be maintained through tools, skills, and procedures that can be managed centrally or via distributed work processes.

Competent resources for the implementation and execution of IDM configuration management shall be provided to perform the required tasks within the defined timeframe.

Criteria for competence shall be established by the IDM program.

6.3 Organization and resources

Management shall provide all resources necessary to achieve and sustain the IDM program.

Management shall specify resource deployment (or organizational structure) including reporting relationships and location.

The IDM program shall be communicated to responsible organizations.

NOTE 1 Resources can be located remote from the facility, can be shared by multiple facilities, and can be supplied by a supplier or contractor.

The enterprise shall identify and document the roles with authority and responsibility to ensure that the functionality and performance objectives for IDM are achieved and maintained.

Resources involved in IDM, such as personnel and toolkits, shall be managed so that they can be used effectively.

Procedures for managing competence (including training) to manage competence of all persons involved in performing one or more roles in the IDM program shall be in place. Skill and competency assessments shall be carried out to document the qualification of individuals against the activities they are performing. Qualified individuals for roles, and changes of an individual within a role, shall be documented.

Each IDM participant shall have the necessary authority and resources to complete their roles and responsibilities.

Enterprise programs should provide processes for sharing technical and management solutions between different organizations covering suppliers and facilities.

NOTE 2 Technical and management solutions include toolkits and templates, work processes, and procedures for management of functionality and performance.

A formal procedure shall be defined for replacing the owner of an IDM work process.

6.4 Developing and maintaining IDM program

An IDM program shall be established and documented to manage long term activities and infrastructure to resolve competing objectives and to manage their priorities.

The owner of an IDM work process shall be assigned to an individual person or to a role.

Replacing the owner of an IDM work process shall consider succession planning and follow the corresponding defined procedure.

The IDM program should be established with consideration for the following topics:

- enterprise risk management programs;
- resource availability;
- quality assurance programs;
- safety program;
- security program;
- enterprise asset management program.

The IDM program shall have a well-defined functional structure.

NOTE 1 An IDM program can provide the organization for management system functions including MOC (see 4.5).

The IDM program shall be defined so that all activities of the different stakeholders involved in the IDM of an enterprise can be effectively coordinated.

The IDM program shall coordinate multiple asynchronous life cycles including facility, devices, technology, and business life cycles as well as the associated work processes.

NOTE 2 IDM will contain some work processes and will also depend on work processes outside of IDM scope.

NOTE 3 IDM can be established at any phase of an enterprise or facility life cycle and can include multiple current and/or future facilities, each at different phases of IDM life cycle.

The IDM program shall be defined by a set of documented management goals, strategies, and objectives.

The IDM program effectiveness shall be continuously monitored and improved.

The IDM program shall be defined so that required resources and accountability are ensured.

The IDM program shall define roles and responsibilities required for IDM. These roles and responsibilities shall be assigned to qualified personnel and/or organizations.

Required competency of each of the roles and associated responsibilities shall be defined to ensure the proper implementation of IDM.

Training programs shall be defined to ensure the competency of personnel for the roles and associated responsibilities to support the IDM program.

NOTE 4 Training programs typically includes, but is not limited to, training on associated hardware, software and procedures.

Training required to support the IDM program and any competency assessments records shall be identified and documented using the facility's designated tools.

NOTE 5 The assessment records can be maintained as per owner's policies.

6.5 Supplier management

6.5.1 Coordination with suppliers

A stable (long term) set of competent suppliers for goods and services that aligns with equipment and technologies used in the facilities shall be established.

NOTE 1 Lack of stability creates a burden on reengineering for MOC and undue risk. A change in supplier can require significant manual reengineering/configuration effort which is error-prone and introduces project risk.

NOTE 2 Stability also provides support for integration with the remainder of the enterprise systems including business systems while also enabling interoperability between host systems and field devices.

NOTE 3 One form of such relationship is a strategic supplier alliance as opposed to an open bidding process for every project procurement cycle.

Suppliers shall be managed based on a documented work process that is routinely reviewed, maintained, and updated.

NOTE 4 Suppliers change during the facility life.

NOTE 5 Life cycles for facilities, devices, and technologies are not synchronized.

6.5.2 Intelligent device life cycle management

A means of managing device life cycle changes shall be provided.

A process/plan supporting product migration shall be in place.

Device life cycle changes shall be planned to minimize disruption to device functionality or performance.

NOTE 1 It is possible that device life cycle changes use the same technology but have changes such as a software revision that forces a change in the device configuration.

Planning and engineering support shall be complete and documented before device life cycle changes are implemented.

NOTE 2 Device life cycle changes can often happen at times other than during plant outages or other facility modifications.

The IDM program shall require device suppliers to provide information necessary for configuration migration between successive device revisions.

NOTE 3 Also see Clause 9.

Unexpected device life cycle changes discovered at installation time are considered as MOC failures. Device life cycle MOC failures should be investigated to eliminate causes of these failures.

Work processes shall be established to ensure that integrity of the design is maintained throughout the intelligent device life cycle.

NOTE 4 Design integrity requires periodically checking and resolving discrepancies between the as designed and currently active (running) configurations.

6.5.3 Device technology life cycle

A means of managing technology change for intelligent devices shall be provided.

NOTE 1 Managing technology change includes planning to minimize disruption.

NOTE 2 Some of the technology management planning including obsolescence planning can be shared with technology suppliers.

NOTE 3 Technology change can be disruptive because of lack of interoperability and incompatibility with host systems.

NOTE 4 Lack of interoperability with host systems can require long term capital improvement plans.

Unmanaged technology obsolescence, which is a MOC failure, should be avoided.

Technology MOC failures shall be investigated to eliminate causes of these failures.

NOTE 5 Technology changes can cause a disruption in device supply.

Each technology related to intelligent devices shall be evaluated carefully before its deployment. This evaluation shall include, as a minimum, the following:

- a) technology maturity and availability (including long term availability);
- b) sources of supply and support including quality and competency;
- c) certifications and approvals.

Engineering support shall be complete and documented before technology changes are implemented.

NOTE 6 Device technology change means a change in communication or sensing technology (e.g., ultrasonic to/from vortex flow) and is separate from technology life cycle changes.

6.6 Developing and maintaining IDM work process templates

Work process templates for IDM should be used.

Where work process templates are used, they shall be defined and documented with minimum content. A work process template shall be defined in a generic way independent of the implementation considering requirements and recommendations specified corresponding to the facility life cycle phase in Clause 8.

Interactions among procedures of every IDM work process shall be specified.

NOTE 1 Swim-lane charts can be used to specify the interactions.

Work process templates shall be maintained and continuously improved.

When an IDM work process template is defined, information common to multiple facilities of the enterprise shall be included.

NOTE 2 This makes IDM work process templates common to multiple facilities of an enterprise.

Each IDM work process template shall identify optional and mandatory provisions for implementation.

IDM work process templates shall be defined to include options for local and remote support.

NOTE 3 Depending on the allocation of responsibilities to local facilities and remote support, contents of the IDM work process templates will differ.

A work process template shall include:

- objective;
- inputs and outputs;
- start timing;
- procedures;
- target facility;
- owner (by role);
- typical roles and responsibilities.

NOTE 4 Inputs and outputs make interactions between IDM work processes clear, since some of inputs are outputs of other IDM work processes.

NOTE 5 Start timing indicates timing at which the IDM work process is initiated.

The IDM program shall define and develop intelligent device templates to manage data in a structured and uniform manner.

The intelligent device template typically includes as a minimum:

- a) tag number (tag number is associated with the application of the device), make and model number;
- b) year of manufacture and serial number (this allows historical tracking of the physical device);
- c) material of construction;
- d) calibrated/instrument range and failure settings (if applicable);
- e) input/output signal;
- f) device power supply and wiring specification (e.g., AC/DC, 2 wire/4 wire);
- g) all other configuration parameters.

NOTE 6 Some devices have additional information like set point, design pressure, body rating, default communication address, etc.

As many templates as necessary shall be developed for each revision of a device type.

NOTE 7 A template for each type of typical device application is normally enough.

NOTE 8 Templates are typically developed, maintained, and provided by suppliers.

6.7 IDM program management and design

6.7.1 Resource management

The IDM program shall provide focus and input to enterprise decisions on resource management including staffing, support tool investments, and budget.

6.7.2 IDM program design and performance improvement

The IDM program shall ensure that general guidelines or templates for IDM programs are customized to fit the enterprise organization.

NOTE Program design can include development of internal work processes and associated training, tools, and development of support from suppliers.

The performance improvement plan(s) shall have systematic data gathering methods and criteria to identify issues/problems and define proper corrective actions.

Performance improvement plans can include program audits or assessments.

6.7.3 IDM program performance feedback to management

IDM programs shall provide metrics to track performance of the overall program, and facility implementations of the program.

NOTE Purpose of performance tracking is to provide formal feedback processes to evaluate overall effectiveness of various elements of the IDM program.

Feedback on performance shall be used to develop work process and/or tool improvements to minimize measured deficiencies.

6.7.4 IDM program operation

IDM programs shall assign resources to deal with:

- changes in the enterprise business model;
- staff changes (such as retirements);
- changes in technology;
- changes in suppliers;
- identified deficiencies in program performance.

NOTE Operation of a program involves ongoing development work which requires resources for the life of the program.

6.7.5 IDM program support and monitoring for facilities

IDM programs shall provide support for IDM in facilities for all facility life cycle phases.

NOTE Support can include documentation, work process templates, training, technology and supplier relationship support, and any other resource that is commonly required by other facilities in an enterprise.

7 Implementing coordination between enterprise, facilities, and suppliers

7.1 Objective

This clause specifies requirements and recommendations for coordination between participants involved in the IDM program including the enterprise, its facilities, and other stakeholders such as intelligent device suppliers.

The coordination includes but is not limited to:

- a) flow of information between program participants;

NOTE Examples of information include but are not limited to device templates, work process templates, problem resolution, and experience (KPIs).

- b) monitoring and improving IDM program;
- c) implementing IDM in facilities;
- d) coordinating suppliers;
- e) monitoring and coordinating IDM activities across/between facilities.

7.2 General

Enterprises shall define boundaries and establish coordination processes for cooperation between IDM program and other enterprise programs as necessary.

7.3 Implementing IDM

7.3.1 Common principles

Enterprises shall implement coordination processes common to multiple facility implementations for IDM program development, review, maintenance, and improvement.

Facilities should set up coordination with suppliers, enterprise IDM program, and other programs. Enterprises shall implement continuous improvement mechanisms for IDM program including audits.

Enterprises shall provide performance metrics and incentives for IDM program.

IDM implementation should be customized to each facility according to its nature.

The effective date of program implementation shall be documented to support periodic audits as established by the quality plan.

NOTE 1 Typically, this will be the "go-live" date of the IDM program.

Each facility shall implement coordination between and across disciplines (electrical, planning, process, operations, etc.).

NOTE 2 This can require modification of existing work processes.

IDM shall be implemented at facilities in accordance with requirements and goals of the IDM program of the enterprise to which the facility belongs.

Basic infrastructure for IDM shall be provided for each facility.

NOTE 3 Infrastructure includes toolkits (i.e., hardware, software) as well as organizational and human resources.

NOTE 4 Common elements of the program are typically available as a suite of options.

Information sharing (problems, opportunities, solutions) between facilities and suppliers shall be implemented.

7.3.2 Implementing IDM in new facilities

Coordination processes for implementing and using IDM support tools and for developing and maintaining procedures for the tools should be provided so that the support tools are used properly and implemented in a consistent way among multiple facilities.

NOTE Introducing new IDM support tools and procedures into a facility is a high-risk activity.

The coordination processes should address the following topics including:

- defining a resourcing strategy including but not limited to
 - selecting IDM supporting strategy from local support and remote support;
 - selecting supporting personnel from facility personnel and supplier personnel;
- selecting IDM support tools including but not limited to
 - deciding on IDM support tools to be used by project and operations/maintenance;
 - determining if existing tools are available and if developing new tools is necessary;

- deciding work processes including but not limited to
 - deciding on IDM work processes necessary for project and operations/maintenance;
 - determining which work process from existing facilities can be reused with or without modification of existing work processes;
 - defining roles and responsibilities;
 - determining roles and responsibilities required for project and operations/maintenance;
 - determining skills to be developed;
 - defining maintenance strategy and implementing the strategy;
- determining, implementing and supplementing management structure for project and long-term support.

IDM tools shall be provided early in the project life cycle (i.e., scope development phase) and not deferred until construction or commissioning.

The scope shall include planning for IDM throughout a facility life cycle.

7.3.3 Implementing IDM in existing facilities

The capability and performance of the currently installed intelligent devices and associated infrastructure shall be determined prior to modifying an existing facility implementing IDM.

NOTE An audit is a commonly used mechanism to determine capability and performance of a facility.

The capability and performance determination shall include all aspects of the existing maintenance program including, as a minimum, equipment, tools, skills and resources, work processes, and procedures.

The IDM implementation plan shall incorporate resolution of all deficiencies noted in the audit.

Maintenance work processes shall be prepared based on the IDM program to achieve desired results at facilities.

7.3.4 Implementing IDM work processes in a facility

The requirement for implementing IDM shall be stated in all Request For Proposals (RFPs), and contracts that relate to or include devices for each facility.

An IDM work process shall be defined by its owner, objective, inputs/outputs, start timing, procedures used and their interactions for a specific facility.

IDM work processes shall be defined and documented for each phase of the facility life cycle of the given facility in accordance with the IDM program of the enterprise.

The IDM work process shall be defined based on the IDM work process template defined in the IDM program considering requirements and recommendations specified in 8.4 through 8.9 corresponding to the facility life cycle phase.

NOTE Work processes are different across facilities. This will result in changes to the generic work process templates used as a basis for the implemented work process.

When a facility develops or enhances an IDM work process, it shall be based on the IDM program with reference to the IDM work process templates defined by the IDM program.

7.4 Coordination for continuous improvement

7.4.1 General

To increase the effectiveness of the IDM program, facilities should share notifications and corresponding solutions for equipment with abnormally high failure rates when they are found.

The IDM program shall include a mechanism for sharing information between facilities.

NOTE 1 Information and experiences can be shared among the enterprise and its facilities to develop and deploy best practices.

NOTE 2 One purpose of information sharing and experiences across the enterprise and its facilities is to develop and implement best practices. Sharing information helps to identify and avoid potential risks.

Procedures shall be created to monitor the effectiveness and performance of IDM in a facility.

NOTE 3 KPIs are an example of a tool to measure monitoring program effectiveness.

NOTE 4 One set of KPIs can be for the effectiveness of program and second set of KPIs can be for effectiveness of implementing IDM in the facility.

The IDM program shall establish quantitative metrics for IDM program performance.

NOTE 5 Quantitative measurements typically include an agreed upon method for capturing the potential impact of incidents avoided as a result of the change in work practices arising from the use of IDM.

The IDM program shall identify and implement opportunities for improving the IDM program, work processes, procedures, or tools.

Facilities shall coordinate and maintain the types and levels of skilled resources to support continuous improvement of IDM.

NOTE 6 Skilled resources include changes caused by shifts in supplier and in-house personnel, supplier contracts, introduction of new tools and technology, and other disruptions of skill requirements.

NOTE 7 Refer to 6.3.

7.4.2 Assessment and audits of IDM activities

Enterprise management shall conduct periodic audits to ensure conformance and compliance to the requirements defined by the IDM program.

NOTE Adherence to objectives and schedules of the IDM program are typical audit criteria.

Reporting mechanisms, such as a dashboard, shall be established.

Non-compliances shall be tracked, reported, and resolved as stipulated in the IDM program quality plan.

Program metrics (for example KPIs) shall be continuously evaluated including review at both the enterprise and facility level.

7.4.3 Resolving causes of program non-compliances

Any non-compliances identified in the audits shall be investigated to determine the root cause of the non-compliance to prevent its recurrence.

Systemic causes of IDM program non-compliances shall be resolved at the enterprise level.

Each facility shall provide initial resolution of local non-compliances and share with others through the continuous improvement process.

NOTE The timeliness of the resolution action can be determined by the importance of the device:

- impact of the device malfunction;
- frequency and/or duration of the device malfunction; and
- costs associated with maintaining the device in an operational state.

7.5 Coordination with other enterprise programs

7.5.1 General

Interactions between enterprise programs shall be fully defined.

Objectives, boundaries, and communication interfaces between affected enterprise program shall be documented.

7.5.2 Life cycle coordination of program activities

Coordination of program activities requires communication between different work processes and organizations reliant on data exchange and the resulting use of the data to support the associated workflows.

All organizations shall coordinate and manage IDM related data transitions required between different data transitions throughout the project and facility's life cycle.

NOTE Applications and associated data can transition between and across different organizations during the life cycle.

7.5.3 Applications

IDM related information should be available for applications to incorporate in their execution.

NOTE 1 This requires identifying IDM related data flows during the early stages of any project incorporating intelligent devices.

EXAMPLE FOUNDATION™ fieldbus¹ propagates and uses device status as part of its field-based control algorithms.

Applications requirements shall be fully defined and shared with IDM for device requirements.

NOTE 2 Applications will define functional, performance, and reliability requirements for devices. IDM is responsible for determining if and how these requirements can be met and resolving differences if they occur.

Applications requirements shall be fully defined and shared with systems, networks, and security for management of IDM.

NOTE 3 Applications will define functional, performance, and reliability requirements for networks. IDM is responsible for determining if and how these requirements can be met and resolving differences if they occur.

7.5.4 Device/process information

Tools that support device information and device configuration should be integrated with systems and applications support tools as well as the overall facility information model.

7.5.5 Systems, networks, and security

Tools and information models that facilitate coordination between the required functionality and risk management, including cybersecurity roles for all participants are required.

¹ FOUNDATION™ fieldbus is a trade name of the FieldComm Group. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products.

NOTE IDM is responsible for determining security information such as access permissions for devices.

7.5.6 Life cycle phases

7.5.6.1 Scope development

IDM tools shall be flexible enough to support required updating to reflect facility changes and to accommodate changes in technology used to support IDM information.

7.5.6.2 EPC

The enterprise shall define mandatory information required as part of the project handover process.

The enterprise should state which data management model is to be used.

EPC organizations shall manage and retain temporary information for the period specified in the contract.

EXAMPLE Shipping and receiving information associated with skid assembly is not required by the facility in operation but is necessary for construction by the EPC.

7.5.6.3 Operate and maintain

A clear data transition plan between each life cycle phase shall be developed.

NOTE Each life cycle phase and participating organization is likely to have different data requirements and potentially different data storage formats.

EXAMPLE Offline by block and build online by individual devices as maintenance is performed.

7.5.7 Application interfaces for coordination

The IDMS shall have an interface to the various software applications used by other roles.

8 Facility life cycle phases

8.1 Objective

This clause specifies requirements and recommendations for achieving and sustaining IDM for each facility life cycle phase.

This clause applies to all facilities where intelligent devices are used.

This clause also specifies requirements and recommendations for management including development and continuous improvement of facility specific IDM tools, work processes, and procedures.

8.2 General

IDM work processes can be executed sequentially or concurrently. Selection of sequential or concurrent execution should be done to optimize allocation of resources.

NOTE 1 The life cycle model in this document shows a simplified linear series of sequential activities. The actual model of a real-life cycle contains a mix of sequential and concurrent activities.

NOTE 2 Many activities require iteration or rework. Iteration or rework when mixed with concurrent work processes creates dependencies between activities.

NOTE 3 Concurrent work can increase the likelihood of errors, omissions, and incomplete work products.

IDM work processes shall support methods for managing concurrent, independent, and dependent work processes.

Rework or iteration shall be complete and documented before a work activity is closed.

IDM work processes for each phase of facility life cycle shall be defined by appropriate timing so that required activities can be done timely and properly.

IDM work processes shall be maintained and continuously improved in accordance with the MOC in the facility.

8.3 Managing facility life cycle phases

8.3.1 General

The life cycle goals, objectives, activities, resources, and status for any endeavour in each facility life cycle phase shall be organized and controlled by a management system.

NOTE 1 Life cycle phases provide a convenient means of communicating life cycle status and actions to affected groups for purpose of managing activities and resources. Life cycle boundaries sometimes overlap or change depending on organizational culture and individual life cycle characteristics.

NOTE 2 Life cycle management is used to determine the requirements for resources and responsibilities for activities that are outside the bounds of normal run and maintain in a facility, and for engineering or design changes within operation and maintenance activities.

Roles and responsibilities for all participants shall be assigned and coordinated throughout the facility life cycle by a management system.

The methodology and responsibility for managing life cycle activities shall be documented and communicated to all participants.

The IDM program shall be implemented to support all life cycle phases, including obsolescence.

A data management system is required to support proper documentation of all life cycle phases.

8.3.2 Life cycle entry points

Facility management processes shall accommodate internally or externally generated changes or disruptions that create a need for work outside the present active facility life cycle phase.

NOTE 1 Changes can come from simple or complex facility modifications, device technology change, or simple device revision migration. Where changes are simple, repetitive, and can be partially automated, the changes can be defined in advance as a work practice or procedure and implemented with minimal impact.

NOTE 2 Some changes such as a device replacement in kind can be completed within a single life cycle phase.

In each case where changes are required, a formal process shall be used to determine which life cycle activities are necessary to support the change and what is the proper life cycle starting point to manage the associated change.

8.3.3 Facility modifications

A proper technical and management review shall be conducted to assess the risk associated with the scope changes before implementing any changes.

Any changes in facility engineering shall be documented, and appropriate training addressing the changes shall be completed before changes are implemented.

A MOC process is required but it can be and often is unique to each enterprise or facility.

NOTE 1 Some facility modifications are simple functional replacements for repair of failed components. Some of these replacements can have very simple life cycle management as defined by facility policies.

NOTE 2 Some of these simple changes can be replicated for many applications of commonly used equipment including common use of engineering and documentation for the replicated changes. IDM programs can assist in replication and sharing.

NOTE 3 Additional information on MOC foundational requirements is provided in 4.5.

8.4 Scope development

8.4.1 General

When exiting from scope development phase to "Design and engineering", the following minimum outputs shall be provided as a minimum:

- intelligent device categories;
- intelligent device management system architecture/block diagram;
- a capability audit of the currently installed intelligent devices and associated infrastructure;
- a list of deviations from the IDM program;
- IDM specific specifications.

NOTE 1 Below is a typical list of specifications affected by IDM that will be required:

- digital instrumentation and valve controller specification – This could be covered in a specific section of the project instrumentation and control valve specifications;
- wireless instrumentation specification;
- intelligent electronic device (IED) specification;
- intelligent device integration and device management system specification;
- OT systems cybersecurity specification.

NOTE 2 The OT systems cybersecurity specification document can be developed by others as part of the broader cybersecurity standards, however the IDM project team also verifies that the document incorporates IDM cybersecurity requirements.

The following IDM work processes shall be defined for the IDM activities executed in the scope development phase:

- planning and design for IDM implementation;
- analysing result of criticality ranking;
- defining long term support strategy (technical support strategy);
- selecting design alternatives;
- preparing tools and (basic work processes) their procedures;
- selecting suppliers;
- developing a cybersecurity strategy;
- planning of handover.

NOTE 3 Provisions for these IDM work processes are specified in the following subclauses.

NOTE 4 Additional IDM work processes could be defined for this facility life cycle phase.

IDM work processes for defining and documenting functionalities of IACS and intelligent devices shall as a minimum be defined for the following operating conditions:

- normal operation;
- abnormal operation; and
- handling faults or failures.

NOTE 5 Work processes and procedures for defining functional requirements are out of scope for this document, but the results of those processes are as required input for IDM.

Requirements shall be defined and documented for IACS and intelligent device performance.

NOTE 6 Performance measures include but are not limited to speed and repeatability.

Requirements and specific plans shall be identified and documented for cybersecurity including compensating work processes and procedures for intelligent devices that do not support cybersecurity.

NOTE 7 Intelligent devices can introduce security vulnerabilities into the IACS.

NOTE 8 Cybersecurity requirements are defined in the IEC 62443 series.

Intelligent devices shall indicate which functions of the device are required for the application.

NOTE 9 A single intelligent device can have many notification configuration options. Failure to include enough detail in the instrument justification for intelligent devices can contribute to alarm and alert flooding during late phases in the project.

NOTE 10 Classification of the notification depends on the role of the device as well as the consequence of the diagnostic information on the operating condition of the device.

NOTE 11 To avoid spurious notifications, functions not indicated in the intelligent device need to be disabled.

IDM tools shall be provided early in the project life cycle (i.e., scope development phase) and not deferred until construction or commissioning.

IDM requirements shall be included in the facility scope development.

NOTE 12 IDM requirements are one component of the entire facility scope.

8.4.2 Objective

The objective of the requirements of 8.4.1 is to categorize the intelligent device applications, including the notifications generated by the intelligent device, in a way that sustainably supports engineering, operations, and maintenance planning IDM activities.

8.4.3 Risk management

8.4.3.1 General

Risk assessment shall be complete and documented prior to IDM design activities.

NOTE 1 Risk assessment is outside the scope of this document and is an important prerequisite of IDM that is conducted during the scope development phase.

NOTE 2 Risk assessment can utilize a variety of techniques including but not limited to: Criticality ranking, LOPA, Fault Tree, and Markov modelling.

NOTE 3 This document does not provide requirements or guidance for these assessment techniques. Other standards such as ISA84 provide guidance.

8.4.3.2 Risk assessment analysis

Risk assessment analysis is used to determine device criticality. The risk assessment analysis shall be completed before detailed design begins.

NOTE Many design choices depend on device criticality. Typically, the IDM program defines rules and methods for the design of intelligent devices covering specific circumstances where consistency is important (e.g., communication protocols) based on criticality ranking.

The approach used in the specification, design, and implementation of an intelligent device shall conform to the defined expectations based on the intelligent device criticality ranking and notification classification for that installation.

The facility specific information about design alternatives shall be retained in a manner that can survive changes in personnel.

8.4.4 Project type considerations

Project scope development and engineering activities shall be tailored to fit the type of project.

NOTE Additional scope development and engineering activities are necessary for facility modification that are not relevant for creating new facilities.

Projects that include modification of existing facilities shall provide assurance that any equipment that will be reused is suitable for the new service conditions.

Design premises and scope development decisions shall be maintained in a manner that supports long term MOC.

If not supported, required infrastructure shall be incorporated into the initial project scope.

8.4.5 Planning and design of the IDM implementation

An IDM implementation plan shall be defined and documented to achieve IDM requirements defined in 9.4.

IDM work process of planning and design for IDM implementation should be defined and executed at the beginning of the scope development phase.

The work process of planning and design IDM implementation shall be consistent with the enterprise IDM program.

The documented IDM implementation plan shall include:

- detailed scope of the IDM implementation;
- IDM work processes to be defined;
- estimated resources required for each facility life cycle phase;
- list of standards, specifications, regulations, and codes applicable to the IDM implementation;
- results of the criticality ranking.

The documented IDM implementation plan can also include:

- KPI formula and target values.

The inputs to IDM work processes of the planning and design IDM implementation shall include:

- objectives of the IDM implementation;
- enterprise IDM program requirements;
- operational philosophy of the facility;
- maintenance philosophy of the facility;
- project execution plan of the facility;
- limitation about resources;
- result of risk assessment.

Additional inputs can include:

- expected performance (KPIs) of IDM.

NOTE A plan to achieve IDM requirements is normally a part of a project plan.

8.4.6 Defining facility long term support plans

If IDM work process of facility long term support plan is not defined in the IDM program, it shall be defined in the IDM work process of planning and design IDM implementation.

A facility long term support plan shall be defined that will sustain compliance with IDM requirements defined in 8.3 for the life of the facility.

Facility long term support plans shall include, as a minimum, local or remote staff resource plans, roles and responsibilities, outside (third party) support, and enterprise support including program level support.

NOTE 1 IDM work processes and procedures will form an essential part of the facility long-term support plan. Some of these work processes and procedures can be supplied by an IDM program.

The output of IDM work process of defining facility long term support plan shall be documented for long term support of intelligent devices.

NOTE 2 The documented facility long term support plan of intelligent devices includes:

- staffing plan about local and/or remote support;
- cooperative local and remote support structure with clear roles and responsibilities for each;
- team charter;
- training and learning paths.

The inputs of IDM work process of defining facility long term support plan shall include:

- facility maintenance program;
- IDM program;
- IDM implementation plan;
- plan of the facility implementation project;
- documented intelligent device criticality ranking strategy.

8.4.7 Handover plan to operations and maintenance

A handover plan shall be defined and documented.

The handover plan shall provide continuity of compliance with requirements.

NOTE Handover represents a natural discontinuity of personnel, tools, work processes and procedures. Handover plans can include training of long-term support personnel and transition to different information management systems.

The handover plan shall:

- a) identify permanent records to be transferred from project to facility;
- b) identify the format of permanent records to be transferred;
- c) provide a complete status of the tasks and the deliverables;
- d) provide a list of activities or action items left open;
- e) outline a list of immediate activities and potential challenges based on the status of the deliverables and open action items.

The documented handover plan related to intelligent devices shall include:

- configuration data;
- templates;
- general handover plan including training and support staff;
- form of documentation and information management;
- MOC/pre-start-up review.

The inputs of IDM work process of handover plan shall include:

- IDM program;
- IDM implementation plan;
- plan of the facility implementation project;
- documented intelligent device criticality ranking strategy;
- documented strategy for long term support of intelligent devices.

The start timing of handover plan should be the point of time where the IDM implementation plan becomes available.

8.4.8 Defining strategy for intelligent device cybersecurity

8.4.8.1 General

The output of IDM work process of developing strategy for cybersecurity shall be a documented strategy for cybersecurity related to intelligent devices.

NOTE 1 IEC 62443 series provides cybersecurity requirements for devices, systems, and procedures or work processes employed in industrial automation.

NOTE 2 These requirements can be simplified with modern tools, or they can be met with manual procedures. The manual procedures can be difficult under some conditions.

NOTE 3 There are no exemptions for devices not designed to provide cybersecurity support tools.

NOTE 4 IEC 62443 series requires a cybersecurity program to ensure effectiveness of cybersecurity measures. IDM is dependent on the effectiveness of the cybersecurity program.

IDM shall provide support for cybersecurity functions including, as a minimum, authentication, authorization, logging, and backup/restore.

8.4.8.2 Authentication

Authentication measures shall prevent anonymous or fraudulent access for software, hardware, or humans.

NOTE 1 Modern components come with certificates and tamper proof storage to ensure authenticity and a chain of trust.

NOTE 2 Modern systems provide role-based log-in with single or multi factor authentication.

NOTE 3 Portable tools do not provide tools to support this requirement and manual procedures fill this void when portable tools are used.

8.4.8.3 Authorization

Authorization shall be employed to provide a means for MOC.

NOTE 1 Authorization is meaningless without authentication.

NOTE 2 Many portable tools do not meet this requirement without manual procedures.

NOTE 3 Manual procedures are generally less effective and more cumbersome than procedures utilizing the correct type and quantities of tools.

Authorization shall provide access control for view and modification of hardware, software, configuration, or operating settings.

Access control shall be provided for devices, systems, and users.

Access control shall be enforced by appropriate tools and procedures.

NOTE 4 Certificates and certificate management systems are a way of ensuring security and authenticity of exchanged data.

Authorization shall be role based.

8.4.8.4 Logging

Logging shall be employed to keep a record of changes.

NOTE 1 Most devices incorporate a change counter to facilitate integrity of this function.

NOTE 2 Many host systems with continuously connected devices can simplify or automat this function.

NOTE 3 This function is more complex and less reliable when the function depends on handheld configuration tools.

8.4.8.5 Backup and restore

Backup and restore functions shall be used to provide a backup of current device configuration and the ability to restore this configuration when necessary.

NOTE 1 Many host systems with continuously connected devices can simplify or automat this function.

NOTE 2 This function is more complex and less reliable when the function depends on handheld configuration tools.

The strategy for cybersecurity inputs shall include:

- facility cybersecurity policies and guidelines for OT domain;
- IDM program;
- IDM implementation plan;
- plan of the facility implementation project;
- documented intelligent device criticality ranking strategy;
- documented strategy for long term support of intelligent devices.

8.4.9 Selecting design alternatives

A design alternative selection strategy shall be documented including:

- grouping of functions;
- approved technologies list;
- design alternatives for each group of functions;
- evaluation criteria for selecting alternatives;
- list of new or untried design practices or equipment designs;
- list of new candidate technologies and industry rate of adoption;
- technology comparison matrices;
- systematic method for retaining the technology evaluation information;
- plan of training and external support for personnel involved in designing and engineering.

The inputs of IDM work process for selecting design alternatives shall include:

- IDM program;
- IDM implementation plan;
- plan of the facility implementation project;
- documented intelligent device criticality ranking strategy;
- documented strategy for long term support of intelligent devices.

Technology selection shall consider the application functional requirement specification and the defined IDM work process, including the requirements for sustainable operability and maintainability.

Selection between design alternatives shall include evaluation of risks as well as benefits of the design or technology choice.

NOTE 1 A choice to "clone" an existing design can lower risk. Alternatively, the cloned design can introduce obsolescence early in the facility life cycle.

Plans for introduction of new technology shall include identification of any needs for new tools, skills, and training and plans for provision of those needs for improvement in existing local infrastructure (green or brown field) and plans to fill identified needs.

NOTE 2 The plan can include IDM program support for introduction of new tools and development of new work processes. Tools and work processes developed outside the facility are often useful.

NOTE 3 Local infrastructure normally includes supply of equipment and services outside the facility that can be used for facility support.

Long term support (i.e., standards as a basis to ensure), maturity model, and stability shall be evaluated in the selection process.

8.4.10 Preparing tools and their procedures

The output of IDM work process of preparing tools and (basic work processes) their procedures shall be:

- tools for IDM;
- procedures to use tools;
- IDM work process for maintaining tools;
- training plans.

Tools for each life cycle phase shall be provided.

Tools shall be able to be used for existing facilities.

The tools should include:

- tool for managing configuration data of intelligent devices;
- tool for configure intelligent devices;
- tool for replacing intelligent devices.

Existing tools can be reused.

A procedure of each tool for each life cycle phase shall be provided.

The training plan of the tools should include:

- training materials;
- milestones in the facility life cycle;
- procedures for managing skills of personnel.

The inputs of "Preparing tools and (basic work processes) their procedures" shall include:

- IDM program;
- IDM implementation plan;
- plan of the facility implementation project;
- documented intelligent device criticality ranking strategy;
- documented strategy for long term support of intelligent devices;
- documented design alternative selection strategy.

System support for export, import, and bulk building (offline - no connected device) of IDM functions shall be considered in IACS design and engineering.

NOTE 1 Bulk building is typically used in large facility implementation projects.

NOTE 2 Use of intelligent device templates or configuration information can support consistency of detailed settings across families of similar devices.

System support for online (connected device) configuration shall be considered in intelligent device system design and engineering.

Engineering and maintenance tools and associated procedures shall be identified and implemented prior to project completion.

NOTE 3 Identified engineering and maintenance tools and associated procedures during scope development will make the design process more efficient and decrease errors of omission.

Requirements shall be defined and documented for a work processes and procedures for device replacement.

NOTE 4 Replacement can be required one or more times during any phase of the life cycle of a facility.

NOTE 5 Replacement devices often contain software upgrades or revisions. A program can provide support for software upgrades or configuration migration.

NOTE 6 Device technology or supplier changes are outside the scope of normal device replacement plans. A program can provide support for technology or supplier changes.

8.4.11 Selecting suppliers

The output of IDM work process of selecting suppliers shall be an approved vendor list (AVL) for each intelligent device category, which can also include recommended model numbers.

This work process shall consider procurement and supply chain requirements.

Each item of the AVL shall include as a minimum the following:

- application type (for example, instrumentation, electrical, process analytics);
- supplier name and contact information;
- intelligent device category (analytical, flow, pressure, temperature, valve, etc.);
- functional groups (major classes of equipment, technology, and/or services).

Requirements shall be defined and documented for supplier choices.

NOTE 1 Items identified as commodities can sometimes be selected after scope development.

NOTE 2 Items requiring engineering effort and IACS integration benefit from early selection and full life cycle support planning.

NOTE 3 Supplier choices can be provided by an IDM program.

8.4.12 Information management planning

Information from scope development and subsequent life cycle phases shall be classified as permanent records or temporary records.

Information identified as a permanent record shall be provided in a form that can be maintained throughout the facility life cycle.

NOTE 1 This life cycle can extend 50+ years and represents a challenge for electronic media. It also represents a challenge for maintaining skills necessary to utilize the information.

NOTE 2 Information management often utilizes different tools, work processes, and skills during different phases of a facility life cycle. Continuity, integrity, and longevity are key for success.

NOTE 3 It is possible that some of the tools and skills necessary for maintaining information are not resident at a facility.

NOTE 4 Intelligent devices require management of significantly more data than older device types.

Information to be managed shall include, as a minimum, data, drawings, calculations, models, and other information and skills necessary to manage and validate design changes throughout the facility life cycle.

A systematic method for retaining intelligent device specification, design (including design alternatives), and implementation information throughout the life cycle of the application shall be established. The method used to retain this information should remain effective despite changes in personnel.

NOTE 5 Establishing a consistent method of documenting details of intelligent device specification, design, and implementation supports success of the IDM project and the long-term integrity of the facility data.

NOTE 6 Refer to Clause 10 for the detail of information management.

8.5 Design and engineering

8.5.1 Objective

The objective of 8.5 is to ensure enough detailed design information is developed to support the procurement, construction, installation, commissioning, operations and maintenance of intelligent devices in a manner consistent with the defined program, management system, and functional specification requirements.

8.5.2 General

Before entering this phase, the following inputs shall be provided:

- a) project scope and objectives;
- b) project/facility standards references, guidelines, and work processes;
- c) project/facility conceptual documents (such as block diagrams, protection strategies and maintenance philosophies);
- d) project/facility preliminary equipment list (instrument index, motor control table, analyser system, etc.).

When exiting from this phase to construction and commissioning, the following outputs shall be provided:

- device management system functional design specification and IACS test plan;
- device list (includes device supplier, model, quantities, etc.);
- device configuration database (which includes datasheets);
- device wiring diagrams and cable schedules;
- network drawings, network block diagrams (communication networks, overall major components, etc.);
- final device criticality ranking (cybersecurity and maintenance) if initial rankings have been changed during design and engineering;
- spare parts strategy aligned with maintenance strategy;
- training and qualifications plan for the facility's team(s);
- device loop-check and commissioning associated workflow diagrams.

The following IDM work processes shall be defined as the IDM activities executed in this facility life cycle phase:

- final supplier selection;
- individual device selection;
- procurement of intelligent devices;
- coordination with related IACS functions;
- specifying work processes for operations and maintenance phase;
- preparation of device configuration templates;
- configuration data preparation (using templates whenever possible);
- configuration verification and testing plans including FAT, SAT.

NOTE 1 Provisions for these IDM work processes are specified in the following subclauses.

Other associated IDM work processes for this facility life cycle phase can be defined in addition to those listed above.

EXAMPLE Presumed supplier's design and anticipated skillsets training.

Detailed configuration management with verification and non-replacement-in-kind shall have a unique intelligent device identifier.

The enterprise shall establish a system for achieving enterprise-wide unique intelligent device identifiers.

NOTE 2 Tag names are one form of unique device identifiers.

Intelligent device detailed configuration design shall provide all configurable intelligent device parameters and associated IACS configuration necessary to achieve the specified functionality.

NOTE 3 Approved intelligent device templates and toolkits, based on the defined criticality rankings, can support the detailed design of the majority of intelligent device parameters.

The intelligent device requirement specification shall enough information to ensure that the detailed design and implementation of the intelligent device achieves the intent and approach documented during the identification, justification, and criticality ranking of the intelligent device.

8.5.3 Device selection

8.5.3.1 General

IDM work process of device selection should be defined before the design and engineering phase starts.

Intelligent device selection criteria shall be defined in the IDM work process of device selection.

Intelligent device selection criteria shall include specified intelligent device and IDM functionality requirements (such as status and diagnostic notifications) necessary to achieve and sustain the required intelligent device and IDM performance in addition to the device's primary function requirements (e.g., primary functions defined by instrument design engineers). IDM requirements shall be stated in the first and all RFPs, and associated contracts that relate to or include devices for each facility.

Requirements for operability, maintainability, diagnostics, inspection and testability shall be addressed during the design of the intelligent device application to reduce the likelihood of dangerous failures.

The output of the device selection IDM work process shall be a list of required intelligent device and IDM functionality for each device type according to its criticality ranking.

NOTE 1 Criticality ranking is described in IEC TR 63082-1:2020, Annex D.

NOTE 2 The device selection activity does not define device criticality itself but specifies the intelligent device functionality (required diagnostic, etc.) for devices of a given criticality.

8.5.3.2 Device selection requirements list

The device selection requirements list shall include:

- description of specific intelligent device functionality(ies);
 - requirements for operability, maintainability, diagnostics, inspection and testability,
 - criteria for selection and principles for design of intelligent devices,
- description of specific IDM functionality(ies);
- device technologies (pressure, temperature, etc.);
- criticality ranking;
- field communications protocols;
- compatibility with the host system is verified;
- when manufacturer/model for the devices are known/shortlisted;
 - manufacturer,
 - model name of the selected device,
 - specification of the device (for example model number, part number to fully describe the device),
 - supplier,
 - tools used for the device,
 - base or optional features (i.e., diagnostics not shown in basic model number),
 - failure handling (e.g., NAMUR NE 043),
 - diagnostics messaging (e.g., NAMUR NE 107),
 - required documentation (e.g., inspection, tools and their usage procedures).

NOTE 1 Consideration of whether new tool types are needed to support the device that the facility is unlikely to have already.

NOTE 2 Available intelligent device and IDM functionality is predetermined when there is only one approved device model for the service/criticality ranking.

When the lists of selected devices are developed, changes to personnel, tools, work processes and procedures should be considered.

Intelligent devices and tools for those devices shall be correctly integrated and configured.

The facility's ability to support each type of intelligent device should be identified and agreed as early in the design process as feasible.

NOTE 3 Selection of devices that are still in development or have new technology for the facility exposes the facility to extra risk that requires special management and testing efforts.

The inputs of IDM work process of "device selection" shall include:

- IDM program;
- IDM implementation plan;
- facility project implementation plan;
- documented intelligent device criticality ranking strategy;
- documented strategy for long term support of intelligent devices;
- functional requirements specification for each type of intelligent device.

The criteria for selection and principles for design should include:

- the role of the host system of intelligent devices in identifying approaches to unsafe or abnormal operation, warning of malfunctions, and prompting an actionable response;
- the methods to be used for intelligent device identification;
- the intelligent device states (e.g., normal, acknowledged, shelved, etc.) that the facility will use.

8.5.4 Procurement of intelligent device

8.5.4.1 General

IDM work process of procurement of intelligent device should be defined as an early input of the design and engineering phase starts.

The detailed design of the intelligent device installation shall be in accordance with the intelligent device functional requirements specification, while also considering the requirements of 8.5.4. The type of device can be sourced from multiple suppliers, the restriction on supplier selection is part of the procurement process.

The enterprise shall identify criteria for selection and principles for design of intelligent devices, consistent with the definition of an intelligent device and the requirements of the IDM program.

The output of IDM work process of procurement of intelligent device shall be the steps to acquire the intelligent devices and associated information for each required device. The associated information shall include:

- manufacturer of purchased device;
- supplier of the purchased device;
- model number of the purchased device;
- unique identifier (e.g., tag number, serial number) of the individual purchased device;
- device configuration information;
- device verification test in shipping container;

- device certification and approval information;
- device support files (e.g., EDD, DTM);
- device service and troubleshooting manuals.

The procurement shall be executed based on the requirements defined by the project and confirmed by the manufacturer.

Configuration of the devices before they arrive on site can be considered. In this case, the device procurement specification should contain the required application-specific information and necessary configuration details.

NOTE If devices are configured prior to arrival on site, the preference is for device configuration confirmation to be performed at the facility prior to final installation.

The inputs of IDM work process of procurement of intelligent device shall include:

- IDM program;
- IDM implementation plan;
- facility implementation project plan
 - project schedule,
 - device location within the facility,
 - list of project standards and specifications;
- list of devices to be procured
 - required certifications,

EXAMPLE Electrical area classification, and special equipment.

- list of functional locations and device identifications for all devices;
- lists of approved device types;
- list of functional location and ultimate ID (e.g., tag name) of all devices;
- compliance with standards for communications, and diagnostic information exchange.

The procurement phase should not start until the list of devices to be procured and the lists of approved device types are ready.

8.5.4.2 Procurement specification

Unique requirements for intelligent devices shall include:

- document;
- requirement for certification;

NOTE Certification can include electrical, safety, communication protocol, and cybersecurity.

- procedure for confirming correctness of parameter setting at time of shipping;
- software revision level.

8.5.5 Configuration data preparation

8.5.5.1 General

IDM work process of configuration data preparation should be defined before the design and engineering phase starts. Configuration data preparation shall include a configuration data verification process to check against design criteria and application to the device.

IDM work process of configuration data preparation shall support the configuration philosophy's intended use case(s) for the configuration of the intelligent devices during the facility's initial construction and commissioning phase and ongoing operations and maintenance phase.

NOTE Configuration use cases can include procurement of factory configured intelligent devices and intelligent devices configured by third parties, e.g., modular units/off site, various onsite pre-commissioning/storage scenarios.

During the configuration process, any proposed modifications shall be subject to an impact analysis to determine:

- the extent of impact on the specified intelligent device functions;
- the extent of testing and verification to be performed or repeated regarding the proposed change.

The IDM configuration process shall provide support for:

- future device revision configuration migration;
- configuration archival and revision logging;
- maintenance management, including maintenance history collection.

The IDM configuration process should provide for remote access intelligent device support.

8.5.5.2 Configuration data preparation inputs and outputs

8.5.5.2.1 General

The inputs of IDM work process of configuration data preparation shall include:

- IDM program objectives;
- IDM implementation plan;
- facility implementation project plan;
- device templates;
- configuration specification for every device.

The start of this step should be the point of time where the device templates and the list of devices to be configured are ready.

The output of IDM work process of configuration data preparation shall be sets of configuration data in a configuration database for every individual intelligent device used with:

- role identifier (tag number);
- set of parameters to be loaded into the intelligent device;
- the device template used for developing the configuration data;
- revision and date information;
- configuration data verification process.

8.5.5.2.2 Intelligent device templates and typicals

Supplier intelligent device templates shall include:

- model name;
- general description of the application type (e.g., pressure, flow, level);
- set of configuration data;
- options for configuration.

When the device templates are developed, discontinuity of personnel, tools, work processes and procedure should be considered.

Device templates shall be maintained to reflect changes in each released revision of a device.

Template "Typicals" should also be prepared for frequently used equipment classes to help ensure consistency and improve efficiency for this design and engineering phase.

NOTE "Typicals" are often based on the supplier templates and are normally user developed.

The design and engineering process shall accommodate changes to the released revision of a device, either by preventing any changes after a certain date or milestone in the project, (for example "freeze date") or by continually updating and maintaining the device templates through to completion and handover.

Each intelligent device's set of configuration data should be prepared based on the corresponding device template.

8.5.5.3 Configuration management

8.5.5.3.1 General

Configuration management shall be part of the IDM program.

NOTE 1 Configuration management work processes can be owned and used by suppliers or by facilities at different times.

IDM configuration management shall include as a minimum the following elements:

- implementation;
- resources;
- work processes; and
- training/competency.

Configuration management shall:

- be designed to integrate with IACS, maintenance management system and other relevant systems in the facility;
- document the approved detailed configuration for the intelligent devices and connected IACSs in the scope of the installation for the life of the intelligent device.

The approved configuration of intelligent devices and connected IACSs shall be subject to MOC practices based on the criticality ranking of the intelligent device.

The intelligent device functional requirements specification shall be expressed and structured in such a way that the specifications:

- are clear, verifiable, and maintainable;
- aid comprehension and interpretation by those who will use the information at any phase of the IDM facility life cycle.

The intelligent device application requirements specification should include application requirements resulting from the criticality ranking, including:

- what to monitor by equipment class;
- the initial classification and priority of each notification; and
- the associated escalation policy.

Configuration data shall include all configuration parameters of all intelligent devices and all parameters associated with the intelligent devices of the IACS.

NOTE 2 These configuration parameters can be classified into the following general categories:

- configuration parameters associated with intelligent device functions;
- configuration parameters associated with intelligent device diagnostics;
- configuration parameters associated with intelligent device communications.

Integration message structures are part of configuration management.

8.5.5.3.2 Implementation

The IDM configuration management practices shall be documented and distributed to IDM participants for performance of IDM activities.

The implementation plan for configuration management should establish specific steps and milestones.

Necessary hardware and software shall be provided to perform configuration management tasks and documentation of their results.

Enough qualified resources shall be regularly allocated to ensure that necessary tasks can be completed.

NOTE 1 This requires resource reconciliation and actions to close any resource gaps identified.

NOTE 2 Intelligent device criticality ranking is key to resource reconciliation.

NOTE 3 The reconciled list of tasks reflects both risk reduction and value creation.

8.5.5.4 Configuration database

The configuration database should include:

- device configuration file – parameter settings in an intelligent device and associated databases;
- control system configuration;

NOTE 1 How the data is received and transmitted to other systems such as the HMI, controllers, and Historian is part of the IACS configuration.

NOTE 2 IACS configuration also includes how the system responds to different types of events.

- HMI presentation – how and which alarms and alerts are presented to the operator or appropriate individual for corrective action;
- tools and systems involved in intelligent device management – what parameters are to be transmitted (directly or indirectly) to systems other than the control system to initiate corrective actions.

The intelligent device and connected IACS shall be configured to respond to intelligent device diagnostic events or other detection of abnormal intelligent device performance as specified in the intelligent device application, including the associated criticality ranking.

NOTE 3 Specified responses can include notification to personnel or automated IACS handling.

8.5.5.5 Configuration specification

The intelligent device configuration specification shall determine and document, at a minimum, the following:

- intelligent device criticality classification (such as safety, control, cybersecurity, quality);

NOTE Based on criticality classification, additional standards could apply. For example, intelligent devices used in SIS will also be within the scope of the IEC 61511 series.

- justification for the device classification;
- intelligent device functions that will be required to meet the requirements of the intended application(s);
- intelligent device interoperability;
- response for each of the intelligent device functions upon internally diagnosed device failure;
- allowable operator or maintenance staff interaction with the intelligent device function(s), including its manual operation or bypassing;
- desired security features to control local or remote interaction with the intelligent device function(s);
- the process conditions that allow safe online testing and repair of the intelligent device.

Procedures shall be developed to address response to detected intelligent device failure. Development of the procedure should consider the following:

- which intelligent device applications to require a more detailed intelligent device response procedure (e.g., based on priority or class);
- what supporting information to include in the intelligent device response procedures (e.g., cause, consequence, corrective action);
- what method to use to access the intelligent device response procedures (e.g., via the human interface).

Procedures shall be developed to address response to intelligent device diagnostic events or other detection of abnormal intelligent device performance. Development of the procedure should consider the following:

- which intelligent device applications to require a more detailed intelligent device response procedure (e.g., based on priority or class);
- what supporting information to include in the intelligent device response procedures (e.g., cause, consequence, corrective action);
- what method to use to access the intelligent device response procedures (e.g., via the human interface).

8.5.5.6 Configuration data verification

8.5.5.6.1 General

The configuration data verification process shall be defined as part of the configuration data preparation to validate design criteria and application to the device.

NOTE 1 The verification process can be based on a paper and/or database, simulation test or other method.

Verification criteria shall include revisions of intelligent device and support files (EDDs, DTMs etc.), accuracy, standards compliance, and interfaces with other systems, as well as individual parameter values.

The configuration data verification process shall accommodate the project's configuration philosophy being used (factory, field, construction, combinations thereof, etc.).

The configuration data verification process should consider the use of bulk edit tools and checks.

NOTE 2 The bulk edit tools are not necessarily dedicated tools and can be a function within or implemented using other office or asset management software. Bulk edit tools avoid individual parameter transfer by automating or semi-automating this process.

NOTE 3 Bulk edit checks can also be used during the operations and maintenance phase to ensure that the configuration of the intelligent device always conforms to the specifications.

8.5.5.6.2 Device acceptance criteria specifications

The intelligent device selection criteria should be used as the basis for the acceptance criteria specifications. The selection criteria to be considered include specified intelligent device and IDM functionality requirements (such as status and diagnostic notifications) necessary to achieve and sustain the required intelligent device and IDM performance in addition to the device's primary function requirements (by others).

Test reports for conformance to relevant standards by corresponding third party organizations shall be incorporated into the device acceptance criteria.

EXAMPLE 1 Fieldbus consortia responsible for communication protocol certification bodies.

EXAMPLE 2 Certification bodies for hazardous area electrical approval.

EXAMPLE 3 Safety certification.

The device acceptance criteria shall also include the general availability of correct device support files (e.g., EDD, FDI, DTM) against specification and IACS requirements.

8.5.6 Implementing and integrating intelligent device functions with IACS

8.5.6.1 General

Intelligent device connectivity to the IDM system is required.

Intelligent devices connected to the IACS require specific considerations as described in the following subclauses.

NOTE 1 Other intelligent device interfaces to the IACS can exist in addition to connections with the IACS such as handheld mobile devices and dedicated intelligent device communication networks.

NOTE 2 Cybersecurity requirements are considered for each of the various IACS connections.

8.5.6.2 IACS architecture

The architecture design should enable "seamless" transfer of data within and between the relevant layers of the IACS and the associated asset management system when possible.

NOTE In this context, seamless means smooth and continuous, with no apparent gaps or differences between layers and information.

The IACS architecture design shall enable remote access and/or remote support as required by the facility/enterprise. The IACS architecture design should consider cloud support including access and cloud application hosting as part of the solution architecture.

The IACS architecture design shall consider the application functional requirement specification and the required IDM work processes.

Requirements for sustainable operability and maintainability shall be included in the IACS architecture design.

The IACS architecture shall incorporate as minimum cybersecurity requirements for the industry in which it is deployed.

8.5.6.3 IACS Interfaces

The IACS interface design shall consider the intelligent device application functional requirements and the defined IDM work processes so that the interface's communications performance meet the project specification.

EXAMPLE Communications performance includes availability and response times.

8.5.6.4 IACS monitoring support functions

Procedures shall be developed to address response to intelligent device failure detected by the IACS. Development of the procedures should consider the following:

- a) which intelligent device applications to require a more detailed intelligent device response procedure (e.g., based on priority or class);
- b) what supporting information to include in the intelligent device response procedures (e.g., cause, consequence, corrective action);
- c) what method to use to access the intelligent device response procedures (e.g., via the human interface).

The procedures should provide for remote access intelligent device support.

8.5.6.5 IACS configuration support functions

See 8.6.5 for IACS considerations on intelligent device revision configuration migration.

8.5.6.6 IACS and device security

A set of cybersecurity procedures for the IACS and associated asset management system should be prepared with aligning to the facility's/enterprise's overall cybersecurity program.

NOTE Many intelligent devices do not inherently include any support tools for cybersecurity. Cybersecurity support for these devices relies on manual process and procedures and/or external tools, devices.

The procedures should be included in the facility's/enterprise's overall cybersecurity program.

The cybersecurity procedures shall comply with relevant cybersecurity standards, for example the IEC 62443 series.

8.5.6.7 IACS field support functions

Authorized changes performed locally on the physical device using tools independent of the IACS (e.g., handheld, communicator, calibrator) shall be capable of updating changes back to IACS.

8.5.6.8 IACS support of maintenance and testing requirements

The IACS shall support the required level of availability for the intelligent device proof test, functional test and validation test.

IACS support shall include intelligent device manual inspection and testing.

The IACS should utilize intelligent device diagnostics to minimize manual testing.

8.5.7 System integration and testing requirements

Testing with typical physical field devices and systems shall be completed prior to generating bulk offline configuration files that will be used in simulated configuration testing.

NOTE 1 Generating configuration files after they have been tested will minimize rework during subsequent life cycle activities.

Typical configurations shall be preserved and replicated for field use, future plant additions, modifications, and audits.

The typical configurations require accompanying documentation explaining choices made and reasons for deviation from default template configuration.

System integration and configuration necessary for IDM support shall be fully tested before field installation.

NOTE 2 Offsite testing (such as FAT) can be and usually is accomplished using simulated or virtual field devices.

NOTE 3 Testing ensures complete and accurate configuration files and HMI displays.

The configuration files used during tests such as FAT shall be retained and used without change until it has been installed on site.

NOTE 4 Many projects refer to this point as a "Freeze Point".

NOTE 5 The conclusion of the FAT has a system of known functionality. No changes are made until the system is reassembled on site to have a stable start point for the next project phase.

NOTE 6 Projects move to a different MOC system at this point in the project so are unable to track or manage changes during the transition.

Detailed requirements for FAT shall follow IEC 62381.

Any functions that do not work as intended during field integration and resulting field changes shall be validated through formal tests and carefully documented through MOC processes.

The MOC starting point shall be based on FAT tested and documented typical configurations.

Final site installation, integration, configuration, and testing (including SAT and SIT per IEC 62381) shall be complete before commencement of integration of field devices and loop check (per IEC 62382).

8.6 Construction and commissioning

8.6.1 General

Previous life cycle phase activities shall be complete as noted for each activity within this phase.

NOTE 1 Some activities such as site staging and construction normally begin before all engineering phase activities are complete.

The construction and commissioning processes are usually organized according to a responsibility assignment matrix (RAM). The RAM shall describe all the IDM specific activities to be performed during construction and commissioning, and the role of each party for each individual activity.

The status of each activity shall be tracked together with the documentation status and all engineering changes.

Completion of commissioning and pre-start-up safety review (PSSR) for one equipment group within a facility can allow operation of that equipment while other equipment groups are still in construction and commissioning.

Planning for and management of construction and commissioning shall allow for life cycle phase overlap when required.

NOTE 2 Additional permitting and management procedures are usually necessary when construction and commissioning activities are conducted in an operating facility or where they can impact an operating facility.

Field work shall be pre-planned and include the sequence of activities to be carried out, roles and responsibilities, and detailed and specific plans of activities execution.

Clause 8 covers a sequence of activities. The following order of the sequence shall be provided for each equipment grouping to ensure integrity of results:

- a) site staging (all the pre-installation work)
 - 1) identification and inventory,
 - 2) spares;
- b) installation;
 - 1) wiring check and power up;
- c) provisioning;
- d) configuration;
- e) loop check and commissioning
 - 1) training of personnel,
 - 2) operating plant tools and test procedures,
 - 3) in service and ready for start-up;
- f) handover
 - 1) documentation (as-built, markups, etc.),
 - 2) maintenance responsibility;
- g) PSSR.

8.6.2 Site staging

During site activities, the first activity should be verifying that the equipment received matches the procurement specification.

Individual equipment items shall be permanently tagged.

Spares shall be identified by equipment type and tagged as spares.

The spare should be stored separately from tagged or assigned inventory.

The equipment storage shall protect the equipment integrity.

The optional activities include a workshop test.

NOTE The workshop test can include: device configuration, function check, calibration check, etc.

8.6.3 Installation

The order of installation follows the site construction plan.

The intelligent device installation shall be in accordance with the detailed design and requirements specification.

Changes to the intelligent device installation should follow the MOC process. Documentation should include but is not limited to plot plants, construction drawings, hook-up drawings, equipment manufacturer installation manual and drawings, and network drawings.

NOTE 1 There are official installation and commissioning guidelines prepared by organization such as fieldbus organizations that serve as guideline to ensure proper intelligent device installation (e.g., protocol specific guidelines).

The intelligent device installation shall follow good installation practices.

Intelligent device communication cable and grounding shall be performed in strict adherence to the engineering documents.

NOTE 2 Training in instrument wiring practices for field installation crew is often required to ensure adherence to engineering requirements.

EXAMPLE Separation of signal and power cables such as not running signal leads along power cabling and using EMC proof glands.

8.6.4 Provisioning

This activity shall be started after the required engineering, documentation, installation, and system implementation information is available.

NOTE 1 This activity is the beginning of final configuration and commissioning and can only be done with full system support and completed engineering.

NOTE 2 This activity will provide an application and a device with necessary identities to complete configuration and commissioning.

NOTE 3 This activity includes joining the field communication network and enables secure communication with systems as necessary.

A formal provisioning procedure shall be used for confirmation of application and device identity including physical and software tagging and installation in the correct location.

Provisioning shall include manual confirmation by field personnel.

Provisioning shall be completed before further steps such as configuration, loop checking, and commissioning.

Completion of provisioning can automatically initiate download of configuration.

8.6.5 Configuration

Procedures that download parameters from a pre-verified database should be provided for configuration.

Manual data entry of intelligent device configuration shall be supplemented with additional procedures to verify the integrity of the data entered.

NOTE 1 Manual data entry is error prone and is not the preferred procedure for configuration. Automated download is preferred when possible.

The intelligent device configuration shall be backed up, and the backup files shall be marked "As Installed" to keep a record of any future configuration changes during commissioning.

NOTE 2 Intelligent devices often have hundreds of configurable parameters.

The intelligent device configuration and notification management tools and work processes shall be complete in time to use intelligent device diagnostics during loop-checking.

Initial use of tools and procedures should be utilized for training of personnel.

The output of IDM work process of configuration shall be all relevant intelligent devices correctly configured and records of configuration work.

A full installation report shall be generated per intelligent device.

The intelligent device installation report shall state the status of the intelligent device and the intelligent device index shall also be updated.

The intelligent device index and the intelligent device reports shall be handed over to the commissioning team to provide guidance in the preparation of the commissioning plan.

8.6.6 Loop-checking and commissioning

SAT and SIT shall be completed prior to performing loop checks.

NOTE 1 SAT and SIT are covered in IEC 62381.

Loop checking shall begin with verification and sign-off of installation, provisioning, and configuration to ensure that all engineering design provisions have been correctly implemented.

A loop function check shall then be completed to ensure that the devices and systems are properly integrated and function as intended.

NOTE 2 Loop function check includes verification of instrument ranges in devices and systems.

Loop function check shall include exercise of all formal test procedures prepared for long term support of facilities.

Loop function check shall be completed and signed off before initiating device commissioning activities.

Commissioning procedures shall be formal and shall include all procedures required for placing devices and loops into operation.

Commissioning procedures shall include activities and tests such as heat tracing, sample systems, process block valves, fill legs, or other final checks or tests as necessary.

Some commissioning procedures (such as sample systems) can depend on process readiness and can require deferral until an appropriate time.

Any deficiencies in installation or documentation shall be corrected before sign-off.

Formal sign-off of commissioning shall be required. This sign-off shall indicate completion of construction activities and readiness of devices, systems, and documentation for PSSR and transition to operations and maintenance.

IDM commissioning procedures shall be completed and identified deficiencies shall be resolved prior to the PSSR (or equivalent activity prior to the end of start-up of a facility).

Participation in loop function check and commissioning should be considered as a training exercise for facility personnel.

The gaps in coverage between personnel from the construction and commissioning phases and staff providing long-term support should be avoided.

NOTE 3 Refer to IEC 62382 for loop checking.

The plan for commissioning should be prepared before configuration of relevant intelligent devices is completed.

The following activities should be considered in the plan of commissioning:

- a) verifying installation and labelling to ensure the right device is installed in the right place;
- b) establishing digital communication with the IACS;
- c) uploading or downloading parameters to ensure database synchronization (backups, etc.) based on which configuration procedure is used;
- d) performing integration and functional test, e.g., loop testing, to ensure the functions work as designed per the authorized version, including testable diagnostic alerts;
- e) transitioning from design change control to operation change control;
- f) final installation to get the device ready for service;
- g) calibration verification (i.e., zero, span, range, etc.);
- h) assessing to ensure operational readiness.

The output of IDM work process of commissioning shall be all relevant intelligent devices verified for the intended applications and records of commissioning work. Intelligent device records, including configuration, settings, and tests performed, shall be maintained with the records of the associated loop.

8.6.7 Training and personnel competency

Personnel who perform work shall be trained in their assigned work processes, procedures and tasks.

A system to track competency by role and by personnel shall be in place.

The requirements of a sustainable training program include:

- assessment of worker competence and skill gaps;
- attainment of necessary competence;
- periodic review and update of training programs; and
- review of requiring training for new intelligent devices including but not limited to work processes, procedures, and tasks.

Training should include familiarization with equipment, tools used to work with the equipment, and specific techniques and standards or templates for application of the devices used in the facility.

Training of personnel on the use of the IDM system who will be involved in operations and maintenance phases should be started prior to, or during, commissioning in order to familiarize them with the new tools.

The IDM training of personnel should be complete in time to use diagnostics during installation and loop-checking and shall be complete prior to handover.

NOTE The training can be conducted separately from loop checking and commissioning, or training can be combined with these activities.

The required troubleshooting skills of individuals shall be defined prior to the operations and maintenance phase of the project.

Training and competency assessment should be conducted before PSSR.

8.6.8 Handover

All relevant IDM engineering and supplier device information should be documented as it is generated. Access to this information should be provided in a timely manner to individuals based on their responsibilities.

Work processes and tools shall be prepared to manage the handover phase of the IDM facility life cycle.

Documentation and other required information shall be provided in a format that site personnel can access, use, and maintain.

A facility shall have plans for accessing, using, and maintaining, information after handover.

8.6.9 PSSR

All maintenance tools, maintenance work processes, maintenance procedures, training, and staff resources shall be in place prior to the PSSR (or equivalent activity) prior to the beginning of start-up of a facility.

All checklists shall be complete, and procedures shall be tested and signed off before PSSR.

NOTE 1 PSSR can be completed for each equipment grouping in a facility that is ready for start-up.

NOTE 2 Completion of PSSR provides assurance that an equipment group is ready for operation.

8.6.10 Startup

Formal IDM procedures shall be established and implemented for the startup phase of a facility life cycle.

NOTE 1 Startup introduces potential hazards that can be different from the hazards in previous life cycle phases. The differences include different types of hazards and severity of consequences.

NOTE 2 Different methods are used to manage operating risk than those used for previous life cycle phases. Operating risk management is active during startup.

When startup is phased or sequential, extra safety and data management procedures shall be in place to manage simultaneous construction and operation activities.

NOTE 3 Simultaneous construction and operation usually requires extra tools and procedures to keep the construction and operation management systems from interfering with each other.

8.7 Operations and maintenance

8.7.1 General

Tools, resources, work processes and procedures shall be provided before entering operations and maintenance phase of facility life cycle necessary to maintain the specified intelligent device application functionality and overall IDM performance requirements in a manner consistent with the requirements of the IDM program.

Each individual application of the intelligent device should be considered when the above tools, resources, work processes, and procedures are prepared.

At a minimum, the following IDM work processes shall be defined for the IDM activities executed in this facility life cycle phase based on the IDM program:

- a) pre-repair processes;
- b) repair processes (including replacement and inventory management);
- c) post-repair processes;
- d) inventory management process.

NOTE Provisions for these IDM work processes are specified in the following subclauses.

The IDM work process should be continuously monitored, evaluated and improved with the use of the MOC work process.

Facility design changes (from complete control system and software upgrades to minor device replacement) during facility operation should be supported and managed through the facility MOC process.

Appropriate types of maintenance processes should be selected and applied to each intelligent device based on the criticality determination.

NOTE Types of maintenance processes include:

- run to failure;
- diagnostics based maintenance;
- automated fault handling;
- scheduled inspection and testing.

Work processes for maintenance shall be prepared based on the IDM program.

The maintenance history shall be collected to analyse the resulting data for trends, improvements, and metrics to determine the effectiveness of the selected maintenance program being implemented.

Maintenance activities shall document the condition of equipment as found, and note if follow up repairs are necessary.

8.7.2 Intelligent device continuous monitoring, problem identification, problem diagnosis processes

8.7.2.1 Intelligent device monitoring

Information about status and condition parameters that are required per the specified configuration for the intelligent device application shall be collected and retained in accordance with the IDM program and the application the intelligent device is used in.

The collection and retaining of device monitoring information should be achieved automatically and continuously, possibly by remote condition monitoring.

Remote access to intelligent devices should be considered for testing of intelligent devices together with local HMI devices.

Intelligent device diagnostic messages should be automatically recorded. If it is realized through the IACS communication system, intelligent device shall be configured to respond to inquiries or to push condition information.

Information on device monitoring should be available through reporting tools with standard degree of analysis capability.

Work processes and procedures should be defined for responsible individual having authority to respond and act on monitoring information, based on criticality ranking and device type parameters to be monitored.

The device supplier should specify the diagnostic coverage of the intelligent device and confirm what diagnostics are actually covered, especially for safety implementations because it impacts the SIL calculations.

The integrity of the configuration of intelligent devices should also be monitored.

The IDM program shall establish a performance monitoring system for intelligent devices.

The enterprise shall identify and implement requirements for communication and management of notifications from intelligent devices about their diagnostic as defined in the IDM program.

NOTE 1 Communication and management of intelligent device diagnostic notifications can be different for the same type of device, depending on the importance of the device's function and the impact of the diagnostic to the device.

NOTE 2 Refer to IEC TR 63082-1:2020, Figure 18.

8.7.2.2 Intelligent device functional testing and inspection

IDM work processes and procedures shall support the inspection and testing requirements specified for the application using the intelligent device.

Testing shall also include process input testing to test full functionality rather than communications function only.

The records, results and documentation from intelligent device functional testing and inspection shall be maintained and stored by the facility. The retention of the records and documentation shall be defined by the enterprise.

8.7.2.3 Intelligent device problem investigation

Work processes and work procedures for investigating problems on intelligent devices shall be developed. These processes and procedures should include metrics to be monitored to detect issues that require further inquiry to identify symptoms.

Calibration, repair, or replacement processes shall be initiated when the investigation identifies what work is required.

8.7.3 Intelligent device calibration

A work process for calibration shall be developed based on device types and technology.

Semi-automated calibration using the supplementary adjusting function of intelligent devices should be considered as a tool for calibration of intelligent devices together with reference signal source through the network.

Semi-automated recording of calibration work using the communication capability of intelligent devices should be considered as a tool for calibration of intelligent devices together with reference signal source through the network.

Calibration also shall include process input testing to test full functionality rather than the communications function only.

8.7.4 Repair processes

8.7.4.1 General

Identified intelligent device failures or revealed degradation shall be corrected within the timing for the specific intelligent device application. In the absence of specific intelligent device application, intelligent device repair or replacement shall be in conformance with the intelligent device criticality ranking.

The intelligent device repair or replacement execution shall be recorded based on facility guidelines for the following purposes:

- maintenance planning;
- reliability analysis;
- inventory control.

8.7.4.2 Loop repair

The work process for loop repair shall be determined based on facility guideline for bringing the loop back to original function.

The loop repair work process can include the following:

- device status is reported;
- notification of device status is made to the operator;
- operator confirms device status and process impact;
- operator reports device status to maintenance;
- intelligent device maintenance performs initial troubleshooting of the device;
- online or offline repair of the device;
- device is returned to functional condition.

Loop repair shall be initiated when failures or degradations of a loop are detected.

NOTE 1 The failures and degradations of loops can be detected through device monitoring, calibration, inspection, and diagnosis.

To identify the cause of the failure or degradation, cause investigation such as troubleshooting should be conducted.

To select a suitable repair process for the situation, risks of leaving the loop as it is and impacts conducting repair should be determined.

A repair process shall be selected based on the cause identified and the result of risk and impact analysis.

NOTE 2 Potential repair processes include configuration change on the host system, configuration change of the intelligent device, firmware upgrading of the intelligent device, repair of connections, and replacing the intelligent device.

If appropriate, the repair can be deferred until the next turnaround. In this case, enough information shall be conveyed to the team for the planning of the turnaround.

Procedure of each type of repair process shall be documented based on the IDM program and the facility guideline.

NOTE 3 Some requirements and recommendations for developing the procedures of types of repair process are specified in the following subclauses.

The selected loop repair shall be executed by following its procedure.

After completion of the repair, a device verification test shall be executed to confirm the repair was correctly executed. If the device verification test is failed, the repair shall be executed again.

After the device verification test, a loop validation test shall be executed to confirm the loop can operate correctly. If the loop validation test is failed, the repair shall be executed again.

8.7.4.3 Intelligent device repair

8.7.4.3.1 Intelligent device hardware repair

The work process shall be determined based on facility guideline for repair of the device. The repair can be executed onsite or offsite.

- Onsite repair should follow manufacturer's recommendation.
- Offsite repair should be executed by repair facility certified by the manufacturer.

8.7.4.3.2 Intelligent device reconfiguration

Configuration data of each intelligent device shall be maintained and updated.

Intelligent device configuration data shall be determined during engineering and design phase and shall be communicated by the host system. Engineering documentation shall be maintained and confirmed within the host system.

Intelligent device reconfiguration shall be implemented when a change to the configuration data is agreed upon at the facility level that determines a different configuration is required.

In preparation for intelligent device reconfiguration, facility shall develop a strategy for implementation including templates, tools, testing, procedure reviews, IACS requirements and documentation.

Remote reconfiguration using the communication capability of intelligent devices should be considered as a tool for reconfiguration of intelligent devices.

NOTE Changing process conditions or maintenance could also affect maintenance diagnostic settings.

Backup and restore data should be done on a regular basis with secure archiving as per good practices.

Reconfiguring intelligent devices shall follow the MOC procedure.

8.7.4.3.3 Intelligent device firmware upgrading

Firmware upgrade(s) for each intelligent device shall be evaluated before implementation.

NOTE 1 A firmware upgrade can have unintended impact of intelligent device performance in a loop. Testing of a firmware upgrade before implementation can be considered as part of the evaluation. Testing of the loop after firmware upgrade to confirm proper operation can also be considered.

Intelligent device firmware upgrade shall be executed by a procedure based on manufacturer release of firmware for an existing intelligent device.

The online firmware upgrading should be considered as a tool for reconfiguring intelligent devices.

The reasons and results of firmware upgrade should be recorded.

MOC per device type instead of application when upgrading to a new revision shall be considered.

NOTE 2 Since the device being upgraded is unavailable during upgrade, the process can be affected, which can require some recommissioning procedures to start-up again.

8.7.5 Intelligent device replacement

8.7.5.1 General

It shall be confirmed that all used functions of the installed intelligent device are covered by the replacing device in advance, during evaluation and prior to replacement. In the case additional functions (e.g., diagnostic function and multi-variables measurement function) are used, their functional details shall be maintained after the replacement.

In addition, interoperability between host systems and the replacing intelligent device shall be evaluated and maintained. The result of the interoperability test provided by the manufacturer of the intelligent device should be used as a part of the evaluation of interoperability between host systems and the intelligent device, if available.

8.7.5.2 Intelligent device replacement engineering

When a notification about a change on intelligent device is announced by the intelligent device manufacturer, impacts of the design change shall be evaluated.

NOTE 1 Changes on intelligent devices can be firmware upgrading, version updating or obsolescence of the model of intelligent device. Alternative solutions for obsolescence by the manufacturer can be a similar intelligent device model from the same manufacturer, a similar intelligent device model from a different manufacturer, or an intelligent device model based on a different technology.

Based on the analysis of the impact of the proposed change, changes to an installed intelligent device shall be managed in accordance with the IDM program MOC requirements and the MOC practices and procedures applicable to the application(s) in which the intelligent device is used.

The evaluation of design changes shall be executed according to an appropriate evaluation procedure depending on the type of design change.

The evaluation shall verify the functionality of any new type of device against the requirements for every use of installed device in terms of hardware and software.

The evaluation and testing shall determine if variations of configuration changes and options are acceptable and if new features are to be used.

Documented evaluation procedures for every type of change shall be provided according to the following subclauses of this document as a part of the IDM program in advance. They should be routinely reviewed and maintained.

Any compatibility issues found during the evaluation shall be resolved.

NOTE 2 The solution can be the modification of configuration data of intelligent device or modifications of the host systems including modification of the application program.

Depending on the result of the desk analysis which is based on intelligent device specification sheets and the evaluation procedure, testing with intelligent device samples shall be conducted.

NOTE 3 The desk analysis determines if a hazard risk assessment is required.

If the evaluation concludes that the design change is not acceptable, proposals of alternative solutions should be requested to the manufacturer.

If the evaluation concludes that the design change is acceptable, documented procedures of intelligent device replacement shall be developed based on facility guideline.

Intelligent device replacement procedures shall follow the facility's MOC process.

The evaluation result shall be documented.

Documentation of the last approved intelligent device hardware revision, firmware revision, embedded software revision, and configuration parameters shall be retained.

NOTE 4 This information is essential to perform the MOC for intelligent devices.

The replacement procedures in terms of model compatibility for every possible combination of installed intelligent device and replacing intelligent device shall be provided.

NOTE 5 Possible combinations between installed intelligent device and replacing intelligent device can be replacing with the same model with same version, replacing with same model with different version, replacing with a different model from the same manufacturer, replacing with a model from different manufacturer or replacing with a model based on a different technology.

The replacement procedures shall take into account modifications of configuration data of the intelligent device and of host systems, including application software.

Semi-automated/automated migration support tools should be used when changing device revisions.

NOTE 6 Each replacement/change option becomes increasingly complex and requires additional MOC.

The replacement procedures shall be routinely reviewed and maintained.

Changes or modifications to the intelligent device shall be documented and archived.

NOTE 7 Modifications need to be entered in the design tools and processed to the new configuration so the updates to the changes are recorded directly after the change is made.

NOTE 8 If the procedure for as built is applicable, it is included as part of the change process.

8.7.5.3 Intelligent device replacement in kind

Before replacement in kind of the intelligent device, the following shall be ensured:

- the model and hardware specifications of the replacing device are maintained the same as those of the installed device;
- the firmware revision and usable toolkit (e.g., EDD file) revision of the replacing intelligent device are the same as those of the installed device; and
- the configuration settings of the replacing device are maintained the same as those of the installed device.

NOTE The configuration setting can be downloaded into the replacing device by the host system.

8.7.5.4 Intelligent device replacement with revised firmware

The appropriate evaluation procedure shall be initiated when a revised firmware version of an intelligent device is released to determine the impact of changes of the revised intelligent device firmware and if a replacement will be implemented.

The evaluation procedure for the revised firmware shall:

- confirm that functionality of the replacing device is compatible with the installed device;
- define the required procedures to replace, if applicable, the current intelligent device with a revised firmware version following manufacturer's guidelines;
- identify the configuration parameters to be set on the replacing device;
- identify the software updates, configuration parameters and data to be set on host systems;
- determine if testing before replacement is necessary, and define the testing procedure as required;
- define the testing procedures after replacement, including device operability and integration with the host system and testing of the associated loop.

8.7.5.5 Intelligent device replacement with different model

In the case the manufacturer of a type of installed devices develops a different model that is a direct replacement of the installed device, each of the installed devices can be replaced with a device of the different model.

8.7.5.6 Intelligent device replacement with different manufacturer

In the case the manufacturer of a type of installed device is not able to continue to provide a direct replacement, a replacement should be found from a different manufacturer.

The manufacturer of the replacing device shall be evaluated (e.g., performance, training, testing tools, manufacturing protocol, spare parts).

8.7.5.7 Intelligent device replacement with different technology

Prior to replacing an intelligent device with a different technology, MOC shall ensure that the original functional scope is covered.

NOTE Different technology in this context means a change in the field device sensing technology.

8.7.5.8 Intelligent device replacement execution

Intelligent device replacement should be considered if device repair or online loop repair is not acceptable.

Intelligent device replacement shall be executed according to the appropriate procedure based on the compatibility situation.

NOTE 1 Situations of compatibility include same model with same version, same model with different version, different model from the same manufacturer, different model from different manufacturer, device based on new technology.

The configuration parameters of the replacing device shall be set correctly according to the replacement procedure.

The parameters on host systems related to the device shall be reconfigured according to the replacement procedure.

After replacement, device verification test shall be executed.

A loop validation test shall be executed based on the facility guideline with the emphasis on the portion of the loop that was replaced.

The result of the replacement shall be recorded in the maintenance records after it is completed.

A work activity record shall be created each time a maintenance activity is performed on an intelligent device.

IDM work process and procedure documentation shall include, as a minimum, the following:

- a) role assignments;
- b) training and competency definition and assessment procedures;
- c) scope and responsibility matrix;
- d) work process specifications;
- e) procedure specifications;
- f) task specifications;
- g) tool certification procedures;
- h) required collection of results and formats, data structure;
- i) communication strategy and protocols;
- j) notification specifications;
- k) access restrictions;
- l) document distribution matrix.

The IDM program shall define the process to determine the suitability of a device for use in accordance with functional safety standards, for example IEC 61511-1.

NOTE 2 Examples include calculation of MTBF using maintenance records.

Related configuration data of the intelligent device and the related host systems shall be updated in the configuration database.

8.7.6 Intelligent device inventory management

A facility inventory strategy shall be developed taking into account device interchangeability.

The number of inventory of replacing intelligent devices and/or spare parts to be kept onsite shall be evaluated. The evaluation shall take into consideration device criticality ranking, delivery lead time and frequency of replacement.

To minimize the inventory cost, the number of replacing intelligent devices and/or spare parts onsite inventory should be managed at optimized levels. Options of intelligent devices allowed to be used should be restricted and software configurable intelligent device types should be selected to reduce the number of types of intelligent device.

Information about firmware revision of every device including device in inventory shall be recorded and updated. To ensure this, a procedure for recording the information shall be documented and maintained.

Upgrading of intelligent devices in inventory should be performed at the time a design change of the intelligent device is accepted after evaluation.

When removing an overhauled intelligent device from inventory, the starting configuration of the intelligent device being removed from inventory shall be confirmed or reset to factory default.

8.7.7 Post-repair processes

8.7.7.1 Reliability analysis ("bad-actor")

Enterprise and facility specific metrics or KPIs for intelligent devices and host systems shall be developed.

The collected intelligent device metrics and KPIs shall be periodically analysed:

- to identify intelligent devices which require maintenance action;
- to identify conditions where there are potential misapplications of intelligent device technology;
- to optimize effectiveness of the maintenance schedule over time; and
- to identify problems and fix worthwhile to share across facility and enterprise.

The analysis method can refer to other standards.

8.7.7.2 Root cause analysis

The work process for performing each type of root cause analysis shall be defined by the enterprise and properly documented within the facility.

The work process shall include:

- limitations and the criteria;
- the triggers for initiating the analysis;
- the personnel with the knowledge, experience, and proper qualifications to perform the analysis;
- the methodology for each type of analysis.

Data from intelligent devices and IDM for analysing and determining the underlying reasons for the fault shall be collected according to the work process.

The data to perform the analysis shall be comprehensive and collected from the following sources:

- diagnostics;
- alarms and alerts;
- trend of process variables (PVs);
- history of operation.

The root cause analysis defined by the work process shall be executed based on the collected data.

The results from the analysis shall include:

- reasons for the fault;
- the process and application conditions related to the failure;
- likelihood of failure;
- statistical error data;
- limitations in the use of device in future applications;
- data to prevent recurrence;
- repair or replacement plan.

A resolution plan shall be prepared to share across facility, enterprise, and potentially the supplier as well. The plan shall include:

- final report of the root cause (failure) analysis;
- communication strategy to share the report across facility, enterprise, and potentially the supplier as well;
- timing for resolution of each action within the plan;
- responsibility assignment.

8.7.7.3 Monitor performance of IDM

The facility shall monitor the performance of the IDM program to continuously improve the IDM program with use of defined KPIs.

8.7.7.4 Planning of scheduled maintenance

The facility shall provide a system to track and schedule routine maintenance for intelligent devices.

The system should take into account the optimization of maintenance interval. Maintenance interval should be based on continuous monitoring, recommendations from supplier, and facility guidance.

8.7.7.5 Turnaround planning

The facility operations and maintenance teams shall provide information to the turnaround planning team.

8.8 Turnarounds

8.8.1 General

Intelligent devices that are affected by turnaround work should be returned to the same stated functionality.

Intelligent device related modifications performed during a turnaround shall follow MOC requirements.

The following IDM work processes shall be defined for the IDM activities executed in this life cycle phase:

- a) preparation for turnaround;
- b) turnaround planning;
- c) turnaround execution;
- d) recommission and start-up.

NOTE 1 Provisions for these IDM work processes are specified in the following subclauses.

NOTE 2 IDM work processes for this life cycle phase can be defined in addition to those listed above.

To reduce turnaround time, the number and duration of actions shall be minimized.

Shared activities in the same area shall be coordinated with other disciplines.

EXAMPLE Installation of scaffolding, unit isolation, insulation, and cladding.

8.8.2 Preparation for turnaround

Preparation for a turnaround shall identify and plan the IDM activities that can only be performed during a facility turnaround or process outage, including:

- diagnostics;
- testing;
- modifications or repairs that can only be performed during a turnaround.

NOTE The turnaround plan incorporates and considers facility maintenance, modification, or capital projects that can only be completed during the brief plant outage period.

Information collected during operations and maintenance phase including intelligent device diagnostic information shall be used to prepare the turnaround plan with enough lead time to allow for engineering design, equipment procurement and execution planning to be complete prior to the start of the outage.

Actions on installed intelligent devices that cannot be accomplished while the facility is in operation shall be planned for the turnaround.

EXAMPLE Valve signature analysis, software program upgrading of computer systems that are related to intelligent device, firmware upgrading, isolation and replacement/decommissioning of equipment.

8.8.3 Turnaround planning

IDM information shall be used to understand intelligent device conditions to determine which equipment requires maintenance during the turnaround.

Turnaround planning shall consider procurement for long lead time items.

EXAMPLE Large valves, special metallurgy.

Turnaround planning shall include identification of required workforce, in particular the need for specialized skills.

The turnaround workforce can include a combination of:

- permanent staff;
- contractors;
- subject matter specialists.

NOTE The turnaround workforce can be a combination of onsite and remote support workers.

The turnaround plan should optimize the required number of workers on site during the turnaround period.

8.8.4 Turnaround execution

Preparation work shall be executed during the operations and maintenance phase before starting the turnaround to minimize the turnaround outage duration.

NOTE 1 Preference is to complete work outside turnaround because of associated complexity and the large number of people involved, which leads to increased risk and associated safety concerns for the workforce.

Firmware and software updates requiring a restart that cause a temporary loss of functionality shall be done during the turnaround phase.

NOTE 2 To prevent a possible unsafe condition, those upgrades requiring a potential restart are done while the facility is in a safe non-operational state.

EXAMPLE 1 Non-redundant processors, safety systems.

NOTE 3 The execution plan includes field devices that can only be calibrated and tested while the facility is in turnaround.

EXAMPLE 2 Axial and radial displacement of compressor sensors, safety system end-to-end checks, valve signatures, pressure safety valves.

8.8.5 Recommission and start-up

IDM commissioning procedures shall be followed for all intelligent devices that are modified, repaired or replaced during a turnaround.

NOTE A PSSR is one typical commissioning procedure.

8.9 Decommissioning

8.9.1 General

Procedures and work processes defining the requirements for intelligent device decommissioning shall be provided.

The facility shall have a decommissioning procedure template to use as a basis for executing the decommissioning work process for each device type.

NOTE 1 The decommissioning procedure is likely to involve skills other than those of the maintenance team.

The decommissioning procedure template shall address each step of the decommissioning process; isolation, cleaning, removal, decontamination and safely return the facility to the operational state.

NOTE 2 The decommissioning procedure template includes all safety and environmental concerns.

The following IDM work processes shall include, as a minimum, the IDM activities executed in this facility life cycle phase:

- a) archiving IDM information;
- b) removal of devices;
- c) refurbishment and/or return to inventory;
- d) disposal.

NOTE 3 Provisions for these IDM work processes are specified in the following subclauses.

8.9.2 Archiving IDM data

Intelligent device decommissioning procedures shall define the requirements for archiving of device configuration and other intelligent device data.

NOTE 1 Regulations can require and dictate which and for how long data associated with the manufacturing process including IDM information is to be retained.

The facility shall maintain a secure database to store archived data.

NOTE 2 The archival database can be stored off site in a secure location.

8.9.3 Removal of devices

All database links referencing the device across the IACS shall be identified, confirmed, and removed if necessary.

NOTE In addition to the control system, the historian(s), maintenance software/tools, field tagging/cabling, P&ID's, operating procedures, and engineering tools/databases are considered as typical links.

The decommissioning procedure template shall include the considerations for physically removing the device from the process.

8.9.4 Refurbishment (for return to inventory)

When an intelligent device is removed and is going to be reused or returned to inventory, the following actions shall be executed:

- a) decontaminate, refurbish, and return to default configuration;

NOTE The normal default configuration is a return to the factory default settings.

- b) verify the intelligent device inventory part number(s) and return the unit(s) to maintenance stores.

8.9.5 Disposal (non-salvage)

Intelligent device capable device(s) shall be returned to factory default configuration prior to disposal.

NOTE Resetting to a generic condition protects intellectual property.

9 Supplier requirements

9.1 Objective

This clause defines recommendations and requirements for suppliers of equipment, software, and services that are utilized or managed by IDM.

NOTE 1 Suppliers can be internal or external to an enterprise.

NOTE 2 End user requirements for the supplier can vary by enterprise.

NOTE 3 This clause clarifies the supplier's role to comply with the requirements of this document.

9.2 General

Products that are for long term applications should be available with support for application portability, interoperability, and migration tools and/or services to manage device life cycles.

NOTE 1 Device life cycles are much shorter than many applications.

NOTE 2 Devices sold for use in short term applications can be sold without long term support.

All products and services shall provide for cybersecurity suitable for the range of expected applications for the products and services.

Unless stated otherwise, requirements specified in Clause 9 shall apply throughout the facility life cycle.

9.3 Products

9.3.1 Devices

In addition to other normal device certifications, enterprises shall require manufacturers to provide intelligent device certifications required for IDM that include, as a minimum, protocol compliance and interoperability.

NOTE 1 Normal certifications include electrical, hazardous area, cyber, safety (SIL), etc. as required.

Installation and application conditions for certification compliance shall be fully described in the documentation supplied by the supplier.

Availability of intelligent device maintenance tools shall be ensured by the suppliers.

NOTE 2 Examples include portable configuration tools, troubleshooting and calibration tools, and software.

An intelligent device shall have its diagnostics capabilities documented.

An intelligent device should be capable of having its firmware updated without losing its configuration.

NOTE 3 For this, provision configuration includes static parameters that define device functionality and performance.

Diagnostics capabilities of each intelligent device shall be documented.

EXAMPLE Diagnostic alerts, communications with maintenance tools, and providing simultaneous process data to control functions are typical types of communications.

All alarms and alerts that each intelligent device can generate, and their default priority shall be documented.

Alarm and alert priority shall be user modifiable.

Devices shall report their condition or state via PV status.

Devices shall report diagnostic conditions via alarms or alerts.

NOTE 4 NAMUR NE 107 defines standard means for PV status reporting and some standard diagnostics reports for some device types.

Devices shall support access control including cybersecurity authentication and authorization.

Devices shall support secure message transmission.

9.3.2 IACS

IACSs shall support device configuration management including:

- new device configuration;
- device replacement including backup and restore;
- device migration to new revisions;
- device support networks, network equipment, and protocols.

The owner operators shall require suppliers to provide a description of how the IACS manages the intelligent device's data base and the intelligent device's configurations.

IACSs shall support device diagnostic notification management and analysis.

IACSs shall support device integration including real time functions and offline functions.

IACSs shall support asynchronous updates of IACSs, portions of IACSs, and devices without disruption of functionality or loss of configuration.

The owner operators shall require the supplier to provide a "system architecture" identifying all the components of the IDM system within their scope.

The owner operators shall require the supplier to document how the IDM system interfaces with other systems such as an ERP, a CMMS, and plant historian.

The owner operators shall require the supplier to document the number of users allowed to use the IACS's functionality simultaneously.

The owner operators shall require the supplier to document the functionality of each IACS component.

IACSs shall provide support for security including support for authentication and role-based authorization for entities including, as a minimum, users, nodes, applications, networks, devices, and messaging.

The IACS shall be capable of handling multiple user profiles. Different user rights shall be capable of being created based on the user profile.

IACSs shall be capable of backup and restore functions for all configuration of nodes, applications, and networks.

The owner operators shall require the IACS supplier to provide a list of all the tested and proved intelligent devices within their scope and to provide documentation describing known problems and how to resolve the known problems.

IACSs shall support monitoring, reporting, logging, and analysis of device and I/O subsystem health.

Work management systems shall treat intelligent devices as individual assets.

Work management systems shall identify intelligent devices by their common identifier.

NOTE 1 The common identifier for many intelligent devices is their TAGNAME as described in ISA5.1.

The IACS shall support firmware version management for all system components and devices.

The IACS shall integrate with the data management and related systems.

NOTE 2 Use of common data and messaging formats is conducive to integration with other systems.

NOTE 3 Related systems can include for Manufacturing Execution Systems (MES), Historians, Enterprise Resource Planning (ERP), Plant Asset Management (PAM), Enterprise Asset Maintenance (EAM), Computerized Maintenance Management System (CMMS), Maintenance Repair and Operations (MRO).

The IACS shall be compatible and able to exchange data with engineering design tools (i.e., computer aided engineering (CAE), smart plant instrumentation, etc.).

9.3.3 Software

The owner operators shall require the supplier to indicate long term support requirements (i.e., expected duration, updates/maintenance) as part of the provided documentation.

The owner operators shall require the supplier to document formal revision management for devices and systems with coordination of revision management for all products and systems offered.

Revision management shall support backward and forward compatibility.

The owner operators shall require the supplier to indicate how to obtain the intelligent device software configuration files securely.

Any software requirements and dependencies on other software shall be documented.

The IDM system software should be modular in design to allow scalability of functionality and devices supported.

Unless stated otherwise, requirements in this subclause can span multiple life cycles.

9.4 Services

9.4.1 Engineering/project support

The owner operator shall require all service suppliers to collaborate with the other suppliers and integrators.

NOTE 1 Typical providers of engineering and project support are: main automation contractor (MAC), main instrument vendor (MIV), individual equipment suppliers, engineering service companies, system integrators (SI), specialty consultants, as well as enterprise and facility support staff.

Formal management of work processes and procedures including formal management of roles and responsibilities shall be developed and followed through all life cycle phases.

NOTE 2 Toolkits and associated templates are one way for providing these formal management systems.

Engineering and project support shall ensure that devices and systems achieve their required level of functionality and performance.

NOTE 3 Functionality and performance requirements, which includes integrating together to work as a common system, are further described in 9.5.

Work processes and procedures shall ensure that the data required by the service supplier(s) is provided. This includes data delivery to the appropriate part of the organization at commissioning/handover.

EXAMPLE Typical data required by multiple users are configuration files, device support files, data sheets, equipment lists, wiring/connection details, etc.

9.4.2 Operations and maintenance support

The facility shall include an ongoing operations and maintenance support plan.

The operations and maintenance support plan shall sustain specified functionality and performance of devices and the associated asset management system(s).

NOTE 1 Ongoing IDM program and device support can be provided by a combination of onsite personnel (dedicated staff and/or contractors), supplemented with remote support by enterprise or contractor subject matter experts.

The operations and maintenance support plan shall be in place prior to start of commissioning and handover.

NOTE 2 The operations and maintenance support plan can be developed by the project for implementation by the facility.

9.4.3 Personnel competency

Cybersecurity measures shall be incorporated in services used in enterprise and facility applications.

NOTE 1 Life cycle phases include consideration of facility and device life cycles.

Personnel competency shall include the required numbers, technical skills, training, and supervision for all work performed.

NOTE 2 Personnel competency in the context of IDM is in addition to, not in lieu of, base competency related to the individual's job role.

Existing enterprise and facility competency program(s) shall incorporate IDM requirements.

The overall competency program shall be updated and maintained according to the IDM program and equipment requirements and changes.

Personnel's IDM competency shall be maintained and qualified.

Competency records should be aligned with enterprise/facility quality standards.

9.4.4 Cybersecurity

Cybersecurity shall be incorporated in the overall enterprise and facility quality programs.

Existing enterprise and facility competency program(s) shall incorporate cybersecurity requirements.

NOTE 1 Third party certification of personnel and equipment is one way of verifying competency.

EXAMPLE Examples of specific items for consideration of cybersecurity competency include but are not limited to:

- demonstrated competency by training on cybersecurity countermeasures and procedures;
- proper handling of equipment protected by cybersecurity countermeasures;
- understanding of applicable industry standards (e.g., IEC 62443 series);
- understanding of IACS and enterprise stewardship standards;
- integrating company policies and procedures regarding cybersecurity control of projects;
- recovery/return to out of box state conditions;
- use of periodic logs/sampling;
- enforcement/improvement of cybersecurity rules.

NOTE 2 It is possible that some aspects of cybersecurity measures are not applicable during particular life cycle phases or tasks.

9.5 Device support tools

9.5.1 Intelligent device templates

The owner operator shall require the intelligent device manufacturer to provide at least one template for each type of intelligent device, according to its application.

NOTE There can be multiple templates for different applications of a common device. For example, a pressure transmitter can be used for level, flow, or pressure.

For each available template, the owner operator shall require the intelligent device manufacturer to identify the intended intelligent device model, intelligent device software revision and intelligent device hardware revision.

The owner operator shall require the intelligent device manufacturer to provide the intelligent device certificate for both the intelligent device itself and its associated templates.

The owner operator shall require the intelligent device manufacturer to identify the default values of the preconfigured parameter settings in the template documentation.

9.5.2 IDM toolkits

IDM toolkits shall enable intelligent device configuration and functionality testing in an environment that will not disrupt the process.

IDM toolkits shall include the bill of materials identifying all software and hardware items.

IDM toolkits shall identify the intelligent device settings that are host specific.

EXAMPLE Host specific settings can be necessary due to proprietary functionality.

9.5.3 Interoperability support of intelligent device management system

IDM software documentation shall include a list of supported communication protocols.

IDM system documentation shall include a list of certifications.

EXAMPLE Certifications include electrical, safety, communication protocols, and cybersecurity.

IDM documentation shall include the device model, software revision and hardware revision for each intelligent device supported and its level of support.

NOTE 1 Results of interoperability testing are useful for engineering, commissioning, and maintenance execution.

NOTE 2 The level of support can be tested and validated by third party organization(s), the IDM system supplier, or some combination of the above.

NOTE 3 Level of support is typically documented in release notes describing any intelligent device functionality limitations due to incompatibilities with the intelligent device.

Intelligent device management system shall support interoperability between monitoring systems and data analytics engines.

9.5.4 Migration, configuration, and maintenance tools

IDM systems shall support backward and forward compatibility to prevent loss of intelligent device configuration during an IDM management system software or intelligent device revision or update.

To prevent the loss of configuration parameters and settings for the intelligent device during a migration, IDM management systems shall allow export and import of intelligent device configuration files generated in a different supplier's IDM management system.

Intelligent device maintenance tools shall support generating full IDM system backups and individual intelligent device backups.

IDM tools and services shall support offline and online device configuration for all necessary life cycle phases.

NOTE 1 Some configuration and migration tools can be used for both maintenance and troubleshooting.

IDM template updates shall be coordinated with each release of the device hardware, software and/or firmware.

NOTE 2 Template update coordination ensures the correct template is used when the device is updated.

10 Information management

10.1 Objective

This clause defines recommendations and requirements for development and maintenance of information management systems.

NOTE 1 The information to be managed includes but is not limited to models, calculations, documents, databases, drawings, configuration files, job role competency and metadata.

This clause applies to:

- suppliers of products and services;
- enterprises; and
- facilities.

NOTE 2 Establishing a consistent method of documenting details of intelligent device specification, design, and implementation supports success of the IDM project and the long-term integrity of the facility.

10.2 General

The structure of IDM shall be fully documented.

The current configuration and all changes to configuration of all intelligent devices and associated information in IACS shall be documented with clear identification of the specified information.

Information shall be managed in a manner that supports achievement and sustainment of required functionality and performance of products and systems over the full life cycle of the facilities where these products and systems are used.

Information shall be managed in a manner that supports product migration and engineering changes without compromising design premises for facilities.

Revision management of the IDM data and records shall be an evergreen process.

NOTE 1 See 10.4 for IDM information.

Information consumers shall be notified about affected records in a timely manner.

NOTE 2 Timeliness is a function of the way in which data is used – Real time, semi-real time, planned. Refer to IEC TR 63082-1:2020, Figure 20.

Information shall be managed in such a way that it can be accessed, used, and updated by responsible personnel.

10.3 Information collection, exchange, reconciliation, and storage

10.3.1 Collection and reconciliation

IDM information collection starts during the project phases. Intelligent device design data, operations and maintenance philosophy, MOC, shall be captured.

The IDM program shall identify and document which information is to be recorded permanently and maintained for the life of the facility.

Each permanent record containing critical information required by IDM shall be uniquely identified and retained.

NOTE 1 A unique identifier (e.g., ISO/IEC 11179-6) enables tracking, and retrieval when required, of each piece of intelligent device information.

All sources of IDM information and consumers shall be fully identified and documented along with tools and procedures, for keeping sources and consumers of information synchronized.

The IDM program shall define and use formal work processes and procedures for information collection and use.

The IDM program shall provide tools and resources necessary to support the work process and associated procedures.

NOTE 2 The identification of information sources identifies the content and syntax of the source and any other metadata necessary to access the information as well as the location.

Temporary and intermediate storage of IDM information shall be identified and documented.

NOTE 3 Intermediate storage is sometimes referred to as a "data lake".

End use repositories of IDM information shall be identified and documented.

NOTE 4 An end use repository can also be a source under some circumstances. Data flow is often bidirectional. For example, an intelligent device configuration downloaded from a central database can be uploaded back to the central database to reflect authorized field changes.

Information flows in the IDM system should be identified and documented.

NOTE 5 This is an established good practice for information management.

Procedures and responsibilities for translating and reconciling IDM information shall be established, executed, and audited for accuracy. These procedures shall maintain the integrity of IDM information.

NOTE 6 Information translation is often required because data formats can differ between sources, data users and intermediate storage.

Information collection processes and procedures shall support, accommodate, and track MOC.

NOTE 7 An example is a design change process using database information as an ongoing process that occurs before field implementation.

NOTE 8 Information collection provides the basis for short term (during a change) and long term (after the change) information management.

Procedures, tools, and responsibilities for migration of IDM information shall be identified and executed when information management systems change during a facility life cycle.

10.3.2 Cybersecurity

All IDM information access and exchange shall use appropriate access control including authentication, authorization, and logging.

NOTE 1 Access control applies to everyone, including third parties.

NOTE 2 Firewalls, data diodes, login management, administrative change logs are appropriate tools for managing data flows and access.

The enterprise shall specify the cybersecurity practices and guidelines to apply to the information management program.

NOTE 3 Representative industry cybersecurity standards include but are not limited to IEC 62443 series, ISO/IEC 27000, and the NIST 800 series cybersecurity framework.

NOTE 4 Industrial cybersecurity is a rapidly evolving field – new support tools, implementations and compliance requirements are probable.

10.3.3 Information storage and retention procedures

The IDM program shall define a comprehensive information storage and retention procedure for the IDM information.

Information storage and retention shall be included in the facility's appropriate quality management system(s) (QMS).

Information storage and retention procedures shall address the migrations between different platforms and in various types and formats.

Information storage and retention procedures shall address the risks associated with access, accuracy, overwrite and retention of legacy information.

The IDM program shall have a procedure for managing storage media that becomes obsolete.

NOTE 1 Hardware, software and media can become obsolete and this can demand migration into a new storage and/or data format.

The records management procedure shall define templates that include the author, level of access and duration of record retention.

The records management shall address the retention of data of different types, formats, and media for storage.

NOTE 2 Storage media can be hard copy, electronic media (CD, DVD etc.), cloud, etc.

Each permanent record containing critical information required by IDM shall be uniquely identified and retained.

NOTE 3 A unique identifier (e.g., ISO/IEC 11179-6) enables tracking, and retrieval when required, of each piece of intelligent device information.

10.3.4 Data management functions

The IDM program shall include establishing a data management program to collect and manage the potentially very large repository of information from diverse sources.

The data management system shall enable structured data exchange.

NOTE 1 This ensures that the right data is available at the right time for the right user.

The data management system shall track and manage different versions of devices.

NOTE 2 This can include hardware and software revisions, replacement and/or retrofit upgrades of devices, work process documentation, etc.

The data management system should organize the data for analysing and reporting the information.

NOTE 3 It is possible that various formats are required depending on the needs of the users (human or machine).

NOTE 4 High level of data integrity helps avoid potentially costly project delays, omissions, and rework.

The data management system should be able to notify changes to data automatically to specific users with relevant information such as what, when, by whom, why and the potential impact.

Alerts shall be sent to specific users of changes to data with relevant information such as what, when, by whom, why and the potential impact.

The back-up strategy for the permanent records and any identified temporary record information shall be identified in the IDM program.

Back up is an action, not an information.

NOTE 5 A back-up strategy can be automatic or manual.

The back-up strategy shall include the:

- back-up schedule;
- information (files, folders, etc.) for back up; and
- back-up location.

If the back-up is manual, the strategy shall also include the responsible person.

NOTE 6 This will help to address data corruption, data tampering and data loss.

Multiple back-ups, if specified, shall be distributed on multiple different physical servers and locations (e.g., on network and off network).

10.4 IDM information

10.4.1 General

The IDM system shall include, as a minimum, the following information which require management:

- intelligent device maintenance and reliability records;
- models and calculations;
- documents and drawings;
- work processes and procedures;
- worker role competency;
- intelligent device configuration management;
- intelligent device templates;
- toolkits.

Each of these information shall include a formal management procedure for their maintenance.

The management procedures shall include a procedure and work process management system with appropriate performance metrics and life cycle tracking.

The record retention period for each type of record shall be defined to align with the facility and regulatory requirements.

Each record shall be executed as defined by the procedure.

10.4.2 Information: Maintenance and reliability records

A work activity record shall be created each time a maintenance activity is performed on an intelligent device.

The IDM program shall define the role(s) responsible, and methodology for, the quality assurance of maintaining the work activity records.

The method and required authority to revise a work activity record shall be defined and documented within the quality assurance process.

Reliability and failure records shall be collected and maintained for each type of intelligent device.

NOTE 1 This information could be shared with external organizations e.g., suppliers.

NOTE 2 Reliability, improvement, design modifications and troubleshooting notes depend on reliability and failure information collection.

Records shall include the application and usage of the device.

NOTE 3 These records permit 'bad actor'/'repeat failure analysis' and application/installation problem reduction.

NOTE 4 Performance indications can be defined using failure records. Failure records can be used to determine the effectiveness of maintenance programs and spare strategy.

10.4.3 Information: Models and calculations

Models and calculations necessary for updating design information shall be maintained and available for use when needed by authorized personnel.

NOTE This information plays a crucial role while designing and executing replacement for non like-for-like intelligent devices, MOC, and design changes.

10.4.4 Information: Documents and drawings

Documents and drawings necessary for long term support shall be kept up to date.

The owner of the document shall be identified.

NOTE The owner is responsible for maintaining the document with the required information, revision control, and access control.

A revision management process shall be used to ensure ready retrieval of the latest revision as well as previous versions when required.

10.4.5 Information: Identification of work processes and procedures

The IDM program shall establish pre-defined, common work processes and procedures for collection, storage, and retrieval of data to ensure smooth data exchange among the various users, prevent data loss and ensure data integrity.

The process for creating, distributing, revising, deleting, and documenting IDM work processes and procedures shall be defined in the QMS and referenced by the IDM program.

10.4.6 Information: Worker role competency

Job role competency details should be managed as part of the IDM system information.

NOTE 1 Competency details includes, but is not limited to, training records, validity date of certifications, skills matrix, etc.

NOTE 2 This requirement also includes personnel assigned from third party service organizations.

Assessment of worker's competency, including assessment process, shall be recorded as defined in the QMS and referenced by the IDM program.

Assessment records shall be retained according to the requirements defined in the QMS, e.g., regulatory quality requirements.

10.4.7 Information: Intelligent device configuration

10.4.7.1 Design of IDM configuration management system

A formally defined system shall be provided to ensure the configuration data is maintained for the software settings of the intelligent devices.

Intelligent device configuration data shall be backed-up and maintained.

The IDM configuration management system shall have appropriate software and/or hard-copy documentation, and work processes to validate for audits.

NOTE Hardware e.g., for intelligent device communication, can be required to perform audit actions.

10.4.7.2 Implementation of IDM configuration management system

The IDM configuration management system implementation shall identify and administer the work process(es) for intelligent device configuration.

The IDM configuration management system implementation shall identify, administer, and integrate the appropriate specialist tools (such as communicators, calibrators) for intelligent device configuration and test.

10.4.7.3 Intelligent device templates

The IDM templates shall be managed as part of the intelligent device information.

NOTE Intelligent device templates can originate and/or be used within and outside the facility. Multiple templates can be associated with a given intelligent device. Templates help to ensure consistent and efficient device specific configuration data initially and during audits.

10.4.8 Information: Toolkits

Toolkits shall be maintained for integration of intelligent devices' data into the common data management system.

NOTE 1 Toolkits typically include all relevant host systems configuration files, 'Wizard' sizing and selection applications (supplier's, and/or company's), etc., including field installation and engineering design work.

Work processes for using toolkits shall also be managed.

The IDM program shall define a toolkit management strategy to encompass both toolkit upgrades and the diverse sources of data.

NOTE 2 The diverse sources of data can typically include the sizing and selection proprietary software/toolkits from the instrument suppliers, safety calculation tools, communication loading tools and cable selections.

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

Annex A (informative)

Clause explanation notes

The numbering in this annex corresponds to the numbering in the main part of the document. This annex is intended to provide context and assistance in the interpretation of the document clauses.

A.4 Foundational requirements for IDM

A.4.1 Objective

Foundational requirements are intended to enable the organization to: 1) implement and sustain an Intelligent Device Management program, 2) to effectively manage intelligent devices themselves, and 3) to gain the full benefit of intelligent devices and connected systems.

A.4.2 General

Foundational requirements which apply to all participants and phases of the life cycle are described in 4.2.

A.4.3 Management functions

IDM like any other initiative or program does not work in isolation but rather aligns with other management functions and programs such as safety and risk management, as well as procedures and processes to document and implement the identified management functions required of the IDM program.

To be successful, IDM like other corporate initiatives also depends on corporate sponsorship, and ownership as well as continuous monitoring to provide accountability.

A.4.4 Formal and informal work process and procedures

Work processes and procedures form the basis for implementation of programs. The IDM program does not work in isolation and integrates with other enterprise initiatives.

Application of processes and procedures requires consistent definition, subjects, criteria, and contents.

A.4.5 Management of change

Change is a constant to be managed and documented.

A.5 Risk management

A.5.1 Objective

Clause 5 provides supporting information and guidance for risk management of intelligent devices and intelligent device management systems.

A.5.2 General

This subclause describes the need for a comprehensive risk management plan in IDM.

A.5.3 IDM program requirements

Programs provide the organizational and management support required to make IDM risk management successful. The IDM program provides continuous support for risk management activities within an enterprise.

A.5.4 Program coordination

IDM risk management cannot be isolated from other enterprise programs. Coordination is required to ensure all programs within an enterprise are synchronized and work together.

A.5.5 Facility level risk management

There are many activities involved in the IDM risk management life cycle. Effective life cycle risk management ensures the coordination of simultaneous and sequential activities from initiation to ending.

Thorough risk identification including all types of event triggers and their cascading effects ensures the effectiveness of the facility risk reduction process throughout the life cycle.

Any changes will be properly reviewed and managed. A change not properly managed will lead to financial, production, schedule delays, resource constraints and other impacts.

Auditing, continuous oversight and monitoring of the IDM risk management process will maintain the integrity of the program throughout the life cycle.

A.5.6 Supplier risk management

A facility needs a consistent reliable supply of products and services throughout the life cycle. All supplier changes and associated risks are to be managed. Managing these risks requires coordination between suppliers, facilities and programs.

A.5.7 Information management risks

Information management brings order and coordination to accessing the information needed for an effective risk management program. Risk management decisions made with inadequate information can lead to improper decisions resulting in higher risk and potential for chaos.

A.5.8 Cybersecurity risk management

Cybersecurity is a critical element of risk management since digital communications are a possible "back door" into the larger IACS environment. Compliance with industry standards and best practices are therefore an important part of any IDM installation and program.

A.6 Enterprise level management for IDM

A.6.1 Objective

An enterprise level management system such as a program provides a means for managing long term activities that compete for resources and often have differing objectives.

A.6.2 General

IDM as a program requires coordination across the enterprise with clear goals and objectives. Specifications, workflows, role descriptions, work processes, procedures, and toolkits/templates are typical ways to communicate and share information to achieve program goals and objectives between all program participants.

IDM support activities are carried out by various suppliers and internal enterprise organizations. These organizations have different goals and budgets and compete for resources. The competition can lead to adversarial relationships that destroy incentives for efficient and effective cooperation and support necessary for IDM success.

Management of IDM is further complicated by device and application complexity as well as continuous change in technology. The use of intelligent devices in industrial automation can increase or decrease application risk depending on the successful management of technical support.

A formally structured IDM program provides resolution of non-aligned objectives and strategies in different internal and external organizations. The resolution can provide for efficient, effective, and cooperative work processes in the various life cycles and organizations. A well-organized program will ensure adequacy of the management processes.

Lack of clearly documented policies can result in confusion regarding program objectives and requirements. Confusion adds risk and expense.

Clearly documented policies provide a means to communicate management goals, strategies, and objectives as well as requirements and recommendations to all participants in IDM. These policies also provide the basis for continuous and periodic performance monitoring.

A.6.3 Organization and resources

The IDM program requires resources, tools, funding, and qualified personnel.

The minimum requirements such as competence, responsibility, and accountability for each of these resources is determined and documented at the enterprise level to ensure a consistent base in all implementations. These minimum enterprise requirements also provide flexibility and career growth opportunities for personnel to redeploy to other program participants (facilities) as needed.

No single source will provide every resource for every facility. No single organization structure will fit the needs of every facility.

Sharing of solutions promotes efficiency and effectiveness of solutions.

A variety of resources provide the means of achieving and sustaining functionality and performance requirements of an application. These resources are available from a variety of organizations internal to an enterprise and from external organizations (suppliers).

Only enterprise management can ensure that resources are available and that they are deployed effectively and efficiently. A program can organize resources in a manner that ensures requirements are met for each type of enterprise and facility.

A.6.4 Developing and maintaining IDM program

Because the IDM program applies across the enterprise, the development and maintenance of the basic requirements are done via a central team of responsible individuals with fully defined roles.

To avoid conflict with other enterprise programs the central team follows the same underlying principles as similar teams within the enterprise. It is the responsibility of this team to resolve differences between IDM and other enterprise programs.

A.6.5 Supplier management

Suppliers are an important part of the IDM program as they provide goods and services on which the IACS is built.

Programs by their nature are long term investments and therefore relationships with key suppliers are also of longer duration than the initial purchase of a device or service as this encourages cooperation between all parties. Examples of this cooperation include suppliers sharing their development plans and soliciting input from their customers.

Similarly, programs require management of each of the life cycles identified in IEC TR 63082-1.

Technology changes are disruptive to a continuous supply of compatible devices to a facility. Device technology changes can cause a need for system changes and can cause a need for supplier changes. Interruptions in supply of products and services required for IDM can occur because of technology changes. Many of these changes are not suitable for management of change procedures designed to address simple product evolution.

Technology and supplier management provides a means to minimize the impact of disruptive changes. Technology migration often requires special measures including upgrade projects. Implementation of technology changes requires long lead time for planning and engineering processes.

As the central part of the enterprise providing continuity to all facilities, the IDM program along with the associated long-term support and development strategy, the central data repository, and the minimum training/competency levels are managed at the enterprise level.

Implementation of the IDM program at facilities will be based on the enterprise IDM program incorporating local practices and regulations.

Intelligent devices are subject to frequent changes during their life cycle. The device revision migration is often specific to a device type and often does not depend on the application where the device is used. Device life cycle revision changes occur asynchronously with facility application changes. Maintenance replacements force facilities to accommodate device revision changes during facility operations.

Many of these changes can be identified, and management of change plans established (in cooperation with the device manufacturer) prior to the use of a new revision of the field-installed device. Migration planning and support can minimize the impact of device revision engineering for normal device replacement. Cooperative work processes and tools allow much of the planning and support to be provided more economically and with higher assurance of configuration integrity compared to independent work performed at each facility.

A.6.6 Developing and maintaining IDM work process templates

Work process templates provide the basis for development of individual work processes at the facilities. Using templates ensures consistency of the safe application of the IDM program while also incorporating best practices as they become available.

A.6.7 IDM program management and design

Management and design of an IDM program is responsible for ensuring its long-term success through provision of:

- Resource management – staff and budget;
- IDM program design and performance improvement for continuous enhancement and effectiveness of the IDM program;
- IDM program performance feedback to management to ensure the program objectives are being met;
- IDM program operations;
- IDM program support and monitoring for facilities while maintaining alignment with the enterprise IDM program.

A.7 Implementing coordination between enterprise, facilities, and suppliers

A.7.1 Objective

IDM programs can span multiple organizations. To be successful, implementation of IDM programs requires good collaboration, good planning, and well-defined work processes and practices. Clause 7 offers guidance to achieve an effective IDM program.

A.7.2 General

How IDM fits with other programs within an organization, as well as how IDM impacts supplier relationships is an important part of an effective IDM program. Understanding the interdependence of organizations within the enterprise as well as interdependence between enterprise and supplier is important to success. Defining these interactive work processes and practices is part of the IDM lifecycle.

A.7.3 Implementing IDM

A.7.3.1 Common principles

This subclause describes the basic requirements for implementing IDM to ensure consistency across the enterprise by enabling coordination and information exchange to implement best practices and for continuous improvement of the associated processes and procedures.

A.7.3.2 Implementing IDM in new facilities

This subclause of the document specifies activities for building teams and projects in realizing project goals by implementing best practices of internal organizational unit(s) as well as external teams through supplier relationships.

This set of activities enables IDM for the full life of the facility.

A.7.3.3 Implementing IDM in existing facilities

Existing facilities will begin by determining the present conditions of their systems and equipment to understand what is required to fulfil IDM requirements. Understanding the present conditions can define the need for infrastructure upgrades, additional resources, and/or improved work processes and procedures in the facility and can also indicate a need for better coordination with outside entities or resources.

A.7.3.4 Implementing IDM work processes in a facility

The IDM program provides a basis for continuity and consistency which drives basic work processes and procedures across the enterprise.

This subclause identifies four basic work process requirements:

- a) IDM as part of purchase and acquisition of equipment and services;
- b) work processes are likely to be different at different phases of the various life cycles but are generally derived from work process templates common to many facilities;
- c) one individual is responsible for the work program;
- d) base or core work process requirements are consistent across the enterprise while also having flexibility to accommodate and align with local work procedures.

EXAMPLE Typical differences between facilities or procedures occur when the work is performed by union or non-union workers, offshore or onshore, local versus remote workers, or geographical differences including language and associated culture.

A.7.4 Coordination for continuous improvement

A.7.4.1 General

Continuous improvement is an important component of better operations, reliability and safety. Communications and sharing lessons learned with all individuals and parties involved are a proven method of ensuring continuous improvement.

Additional mechanisms to determine the effectiveness and benefits of a program include regularly updated and monitored metrics to ensure the right skills are used to support all aspects of the IDM program work.

A.7.4.2 Assessments and audits of IDM activities

KPIs, dashboards, and audits are commonly used methods to measure the effectiveness of work processes, procedures and other program elements against associated requirements. Metrics and feedback can then be used to develop recommended methods for improvement across all program participants. Because audits provide proper documentation, the associated improvements and reasons for the change are also captured.

A.7.4.3 Resolving causes of program non-compliances

An important element in continuous improvement is resolving problems and opportunities identified through self-assessment and audits, then sharing the associated learnings with other IDM program participants.

A.7.5 Coordination with other enterprise programs

A.7.5.1 General

Different programs often work independently to develop information and use their management tools for their internal efforts. These independent efforts need coordination to ensure that all program's efforts fit together.

Unambiguously defined and well understood interactions and interfaces support integration of the IDM program with other enterprise programs without which the full benefits of IDM cannot be achieved.

A.7.5.2 Life cycle coordination of program activities

Applications and associated data can transition between and across different organizations during the life cycle. This requires coordination of how IDM related information is made available outside the IDM program.

Data and application integration is not possible without clear definition of requirements along with agreements on how the data will be shared (i.e. APIs and data format.)

A.7.5.3 Applications

Each program is affected by changes in personnel and management tools as the lifecycle progresses. Data continues to be generated throughout the facility lifecycle from scope development to decommissioning. Managing the transitions, particularly between external organizations and suppliers, are to be managed with the same care and integrity as applications and data are managed.

A.7.5.4 Device/process information

A fully defined application interface makes it possible for other applications and programs to access the data available from the IDMS.

A.8 Facility life cycle phases

A.8.1 Objective

IDM is most impactful at the facility level. Guidance to ensure maximum impact for each phase of the life cycle is provided in this annex.

A.8.2 General

Clause 8 is an introduction to the common requirements for implementing IDM in one or more facilities as part of a broader IDM program.

Depending on the type and scope of work being done, it is often broken into smaller tasks. These tasks can be divided across many individuals or teams and be done concurrently. Tasks are then assembled in sequence to complete the work scope.

Almost all tasks will have some form of recycle, from as simple as corrections as part of a quality assurance process to complete repetition of the task due to changes in scope.

Work processes support the separation into smaller tasks, reintegration into the whole, including any necessary review and recycle.

A.8.3 Managing facility life cycle phases

A.8.3.1 General

Life cycles are generally drawn as a simple linear series of phases. However, many facility activities do not involve all life cycle phases or all activities within the different facility or enterprise life cycle phases.

NOTE Small maintenance or repair projects do not require the same rigour as large expansion or grass root projects.

A management system can determine what life cycle activities and resources are appropriate for a particular initiative or project and thus provide a suitable management system and resources for those activities.

A.8.3.2 Life cycle entry points

Projects come in many shapes and sizes.

A life cycle management system can determine the applicable life cycle entry point for a new activity. For example, many activities skip the scope development phase because the activity or opportunity does not affect the facility scope or risk.

A.8.3.3 Facility modifications

Modifications come from many sources; as small as device revisions, as large as a facility technology refresh, or addition/expansion of the facilities themselves.

The life cycle management system can determine whether design changes can be copied from other similar changes, or whether changes require more extensive review. The management system can also determine the amount of documentation and training required to ensure satisfactory completion before implementation.

A.8.4 Scope development

A.8.4.1 General

Without a scope of work, a project will face risks of changed orders, late changes, non-compliances and over budget execution.

Incorporating the following key factors into the project from the beginning will ensure they are applied consistently while forming the underlying basis for all the elements required of an IDM program:

- a) conformance to IDM program requirements;
- b) interactions between IDM and other standards applicable to the specific application;
- c) ability of the intelligent device to perform the functions relevant to the specific application;
- d) criticality ranking of the intelligent device;
- e) installation and commissioning of the intelligent device, including the intelligent device functions specified for the application;
- f) operation response to intelligent device notifications;
- g) intelligent device maintenance;
- h) monitoring intelligent device performance;
- i) MOC to the intelligent device, the configuration thereof, or the communication system that the signals of the intelligent device are carried through;
- j) long term support strategy.

At the beginning of the scope development phase, the following inputs are expected to be provided:

- a) existing IDM program documents;
- b) intelligent devices applications and deployment philosophy,
 - 1) instrumentation,
 - 2) process control,
 - 3) electrical;
- c) digital instrumentation and valve controllers selection guidelines;
- d) intelligent electronic device (IED) selection guidelines;
- e) site reliability and maintainability philosophy;
- f) network design guidelines for OT systems;

- g) data flow diagrams for IDM system;
- h) OT systems cybersecurity philosophy – it is provided by others;
- i) front end loading – economic benefits and feasibility study of employing digital solutions;
- j) basic infrastructure for IDM.

A.8.4.2 Objective

The objective of scope development is to ensure smooth completion of the IDM program from inception to final implementation and to ensure integrity of the information, details, specifications, and documentation throughout the project.

A.8.4.3 Risk management

IDM is responsible for implementing and maintaining some parts of the enterprise risk management. To accomplish this responsibility, IDM will coordinate with risk assessment personnel to ensure assessors have the information necessary on intelligent devices and their capabilities, and to get the results from risk assessments to fulfil IDM responsibilities.

A.8.4.4 Project type considerations

It is important to understand what type of project is going to be executed: new installation or existing installation.

The type of project will require different considerations to be evaluated during the development of the scope of work.

The following is a list of examples of recommendations for existing installations of intelligent devices.

- a) When an existing intelligent device or IACS equipment will be reused, the project verifies the original design including "as-built" modifications.
- b) When an existing intelligent device or IACS equipment will be reused, the project verifies the current conditions including, but not limited to, non-functioning items, degradation, or deviations from design and obsolescence of hardware or software.
- c) When an existing intelligent device or IACS equipment will be reused, the project determines if it is necessary to create new "as-built" documents, or if available documentation is complete to execute the project.

A.8.4.5 Planning and design of the IDM implementation

This subclause describes the activities recommended for a thorough planning and the implementation of an IDM program.

A.8.4.6 Defining facility long term support plans

This subclause provides a list of recommendations to ensure sustainable operation of intelligent devices and their benefits.

A.8.4.7 Handover plan to operation and maintenance

This subclause provides guidance related to the planning and takeover by the operations and maintenance groups.

The following is a list of recommended information to be included in the handover plan:

- configuration data;
- templates;
- general handover plan including training and support staff;

- form of documentation and information management;
- MOC/pre-start-up review.

A.8.4.8 Defining strategy for intelligent device cybersecurity

This subclause provides reference to the relevant cybersecurity standards in the process industries.

ISA99 and ISA TR84.00.09 provide guidance for the planning and implementation of cybersecurity measures for IACS.

A.8.4.9 Selecting design alternatives

This subclause provides guidance related to the evaluation of intelligent device technologies and their alternatives.

Every alternative considered for implementation is documented for comparison purposes.

The documented design alternative selection strategy can include:

- grouping of functions;
- approved technologies list;
- design alternatives for each group of functions;
- evaluation criteria for selecting alternatives;
- list of new or untried design practices or equipment designs;
- list of new candidate technologies and industry rate of adoption;
- approved technologies list;
- technology comparison matrices;
- systematic method for retaining the technology evaluation information;
- plan of training and external support for personnel involved in designing and engineering.

A.8.4.10 Preparing tools and their procedures

This subclause describes the necessary tools for the successful implementation of intelligent devices and an IDM program.

A.8.4.11 Selecting suppliers

This subclause provides guidance on evaluation and selection intelligent device suppliers.

A.8.4.12 Information management planning

This subclause provides general guidance for the management of IDM related documents and other information.

A.8.5 Design and engineering

A.8.5.1 Objective

The design and engineering processes are critical to the overall outcome for the IDM program. Support and guidance for design and engineering is provided here.

A.8.5.2 General

This subclause defines what is needed from previous phases to get started on the design and engineering phase, and what is delivered to subsequent phases.

This subclause provides guidance to gain clear understanding of the scope of work, objectives of implementing intelligent devices at the facility and ensure that all necessary design inputs are available prior to start detailed engineering.

A.8.5.3 Device selection

This subclause addresses the unique intelligent device requirement to be incorporated into the design documents for device selection.

NOTE Initial device criticality ranking is determined in a prior phase. Design and engineering activities in this phase could result in changes to the initial criticality ranking of a device.

A.8.5.4 Procurement of intelligent device

The unique intelligent device requirements for facility/enterprise procurement practices are defined in 8.5.4.

A.8.5.5 Configuration data preparation

This subclause includes confirmation as well as preparation of IDM data, such as the use of tools (e.g., templates) in data preparation, and the configuration/management of the database.

The subclause also covers verification requirements of the data and acceptance criteria for intelligent devices, which include certification/compliance for the relevant communication protocol, and the necessary support files for the specific device model/revision.

A.8.5.6 Implementing and integrating intelligent device functions with IACS

Intelligent devices require replacement for a number of reasons: failure, obsolescence, or additional functionality required of the application the device is supporting.

A.8.5.7 System integration and testing requirements

Testing that all the components of the system work together is a requirement for complex systems and a factory acceptance test (FAT) is the most commonly used method of achieving the required level of assurance prior to field execution.

Results of this testing also enable the final tuning of the practices, procedures, and implementation details.

Additional information on FAT can be found in IEC 62381.

A.8.6 Construction and commissioning

A.8.6.1 General

This subclause describes the importance of a thorough planning ahead of the construction and commissioning phase.

It outlines the activities necessary to consider during the planning and execution of the construction and commissioning phase.

A.8.6.2 Site staging

The site staging activity ensures that all the resources are available at site and allows equipment to be tested for basic functionality prior its installation at its final location.

A.8.6.3 Installation

The purpose of this subclause is to provide information regarding installation best practices and standards.

Multiple organizations have developed documentation that provides information on how to correctly install intelligent devices to ensure that they perform correctly.

Table A.1 gives examples of such standards.

Table A.1 – Installation guideline documents

IEC 62381
IEC 62382
IEC 61918
IEC 60793-1-40:2019
NEC 250

A.8.6.4 Provisioning

Provisioning supplies identities necessary for cybersecurity, application support, device configuration, network addressing, and other identities associated with a device as necessary. This activity is necessary before other configuration and commissioning activities can proceed.

A.8.6.5 Configuration

Intelligent devices have access to significantly more data and hence parameters and capabilities than traditional devices. The purpose of IDM is to maximize the use of this data and with configuration being the process by which the devices are set-up and connected to the IACS, it is a critical component of the success of the overall effort.

This subclause describes the process that involves the intelligent device configuration download using the files generated during the engineering phase and additional information in case manual adjustments are necessary.

A.8.6.6 Loop-checking and commissioning

IDM changes the way loops and systems are commissioned as there is additional information to be checked yet this additional information can also streamline the commissioning process.

This subclause provides information to plan and execute the loop checking activity of intelligent devices.

The IEC 62382 provides further detailed information and guidance not covered in this document.

A.8.6.7 Training and personnel competency

The intent of this subclause is to assist in the planning and development of training paths to ensure that the personnel assigned to installation and commissioning activities are skilled and capable of performing the job minimizing human errors.

A.8.6.8 Handover

This subclause briefly describes how to conduct a handover of equipment and documentation to the operations and maintenance groups.

A.8.6.9 PSSR

This subclause describes the process of pre-startup safety review and its checklists.

A.8.6.10 Startup

Startup represents the final transition from design/construction to operations which introduces unique risks and challenges. Startup is also when the IDM program formally begins.

A.8.7 Operations and maintenance

A.8.7.1 General

Some repairs require a turnaround to complete and are therefore submitted to the turnaround planning team for inclusion in the shutdown preparation activities.

A.8.7.2 Intelligent device continuous monitoring, problem identification, problem diagnosis processes

Continuous monitoring and analysis of intelligent device diagnostic messages integrated with reporting tools linked to work processes and procedures that are integrated into the IACS and IDMS form the basis of a successful IDM program.

Typical IDM work processes and procedures to realize the value of an IDM program include:

- inspection and functional testing to verify the intelligent device is functioning as it should;
- metrics to identify when an intelligent device will soon require work be done to maintain it within operational limits; and
- data with supporting work processes to determine the root cause of failures when they do occur.

A.8.7.3 Intelligent device calibration

IDM supports the calibration process along with the resulting improvements in the performance of the overall process system. Capabilities of the IACS are to be considered when attempting to develop partial automation of the calibration process for intelligent devices. In addition, all peripheral or supporting maintenance work practices are aligned with chosen calibration methods for IDM.

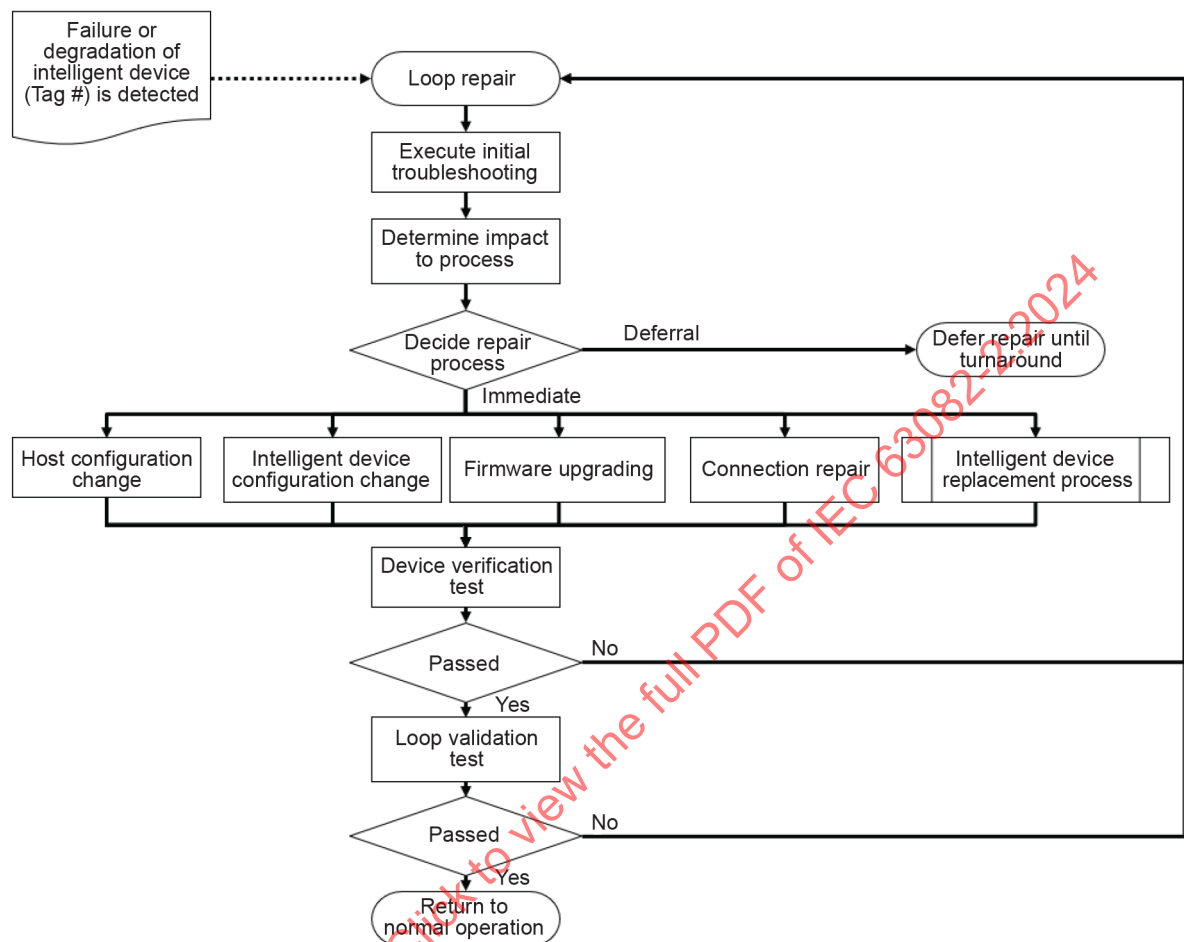
A.8.7.4 Repair processes

A.8.7.4.1 General

Using an IDMS to gather data, analyse intelligent device health and performance, and identify intelligent device degradation over time forms the basis for justification of the IDM program and consequently the associated repair processes used to support the required level of reliability for the process itself as determined by the criticality ranking.

A.8.7.4.2 Loop repair

Figure A.1 shows the overview of the loop repair process for a facility in which intelligent device information is available.



IEC

Figure A.1 – Overview of loop repair process

A.8.7.4.3 Intelligent device repair

As shown in the centre of Figure A.1, once a decision has been made that repairs are required, the resulting work order to execute the repair can impact the following parts of the intelligent device / IACS:

- configuration change of the device and/or host;

NOTE Proper operation of an intelligent device needs that the configuration settings in the host and the device stay aligned.

- intelligent device firmware upgrade;
- repair of the physical connections of the device to the process or communications infrastructure; and
- replacement of the device when repair is not feasible.

A.8.7.5 Intelligent device replacement

A.8.7.5.1 General

Figure A.2 shows the overview of the intelligent device new design evaluation process, the intelligent device replacement process, and how the device replacement process integrates with the loop repair (IDM tools) on the left and the intelligent device suppliers on the right.

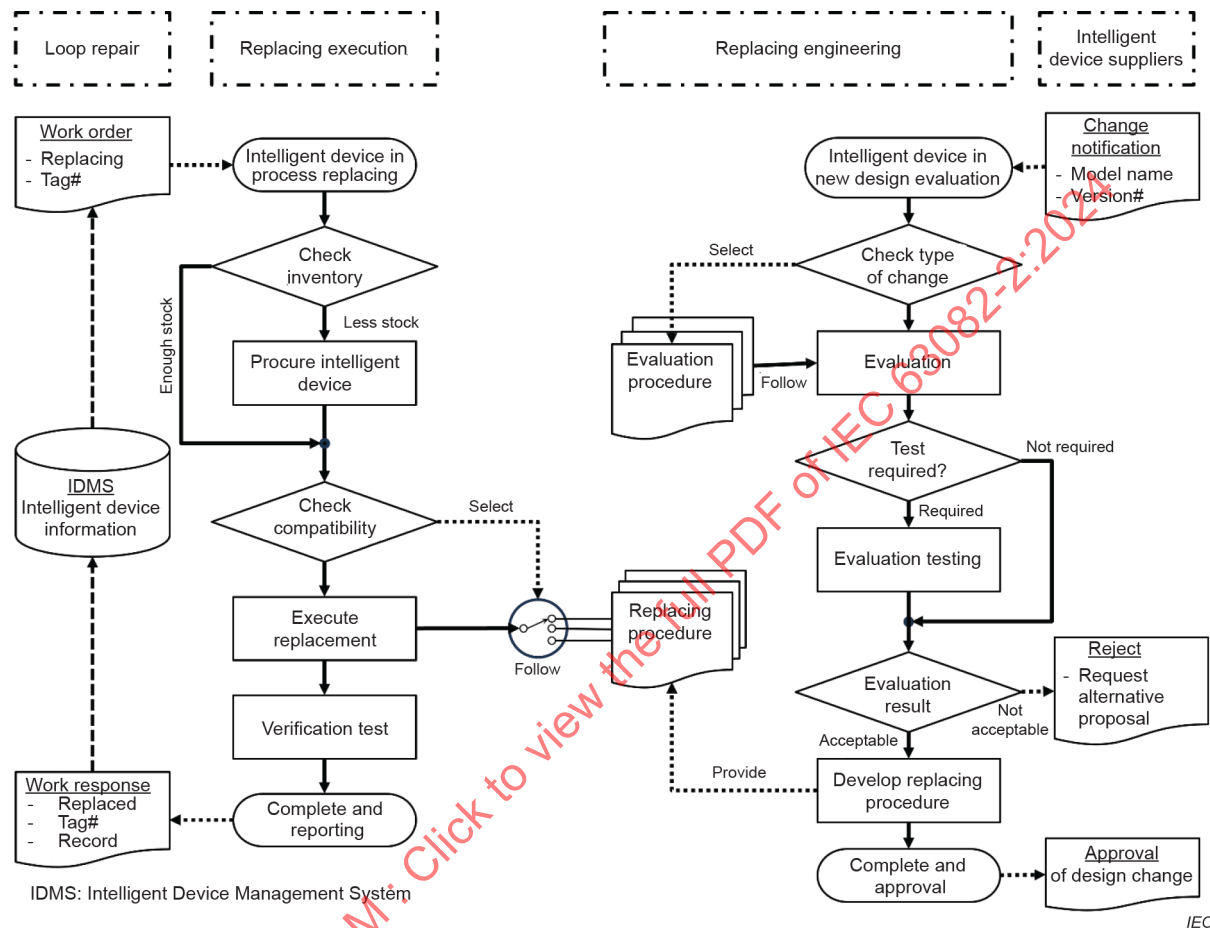


Figure A.2 – Overview of new design evaluation and intelligent device replacement

A.8.7.6 Intelligent device inventory management

Intelligent devices in addition to their enhanced diagnostic capabilities also have the flexibility to have their functionality changed by altering the configuration. The result of this flexibility in how the devices can be used is that inventory management also changes since individual physical intelligent devices can now be used for different applications resulting in fewer devices and reduced inventory and lower costs.

Firmware and configuration management to align with the IACS capabilities now also becomes considered adding a new variable and complexity to the inventory management process.

A.8.7.7 Post-repair processes

An IDM program and integrated IDMS support the automated and semi-automated (human data entry required) gathering of changes made to intelligent devices. Effective use of the resulting data supports subsequent analysis for determination of:

- root causes of failures;
- IDM performance improvements;
- revision of maintenance practices;
- facility outage planning and scheduling.

These activities lead to improved facility operations through reduction in operational and maintenance expense as well as an increase in facility reliability.

A.8.8 Turnarounds

A.8.8.1 General

Turnarounds are a significant phase in a facility life cycle, representing a period during which only certain tasks can be completed. Because shutdown tasks have unique requirements and only occur at low frequency, they require significant planning, which is where intelligent device diagnostic information can provide large benefits.

A.8.8.2 Preparation for turnaround

Preparation for turnaround often begins with data collection and identification of future tasks during the previous turnaround. Performance of tasks such as end-to-end testing of safety systems and identification of equipment for which replacement cannot be procured during the outage window or for which wear and tear data are used to forecast work items for the next opportunity/turnaround.

A key part of preparation is the collection and analysis of data, including information on intelligent device/IDM which can be gathered during plant operation.

A.8.8.3 Turnaround planning

Planning is a multidisciplinary effort with instrumentation and controls being only a small part of the overall plan.

Some parts of the control system typically keep always operating at all times so planning of every action is coordinated into the full turnaround schedule.

NOTE The planning phase normally includes a "freeze date" after which no further items can be added to the turnaround activities/schedule.

A.8.8.4 Turnaround execution

Because so many other activities and resources are being consumed during the outage period, as much work possible and within the limits of tolerable risk, is normally done outside the turnaround window. Those tasks needing an outage include certain software/firmware upgrades requiring a reboot, equipment/device/hardware replacement, and as indicated above certain types of testing.

A.8.8.5 Recommissioning and startup

After turnaround activities are complete, the last step is to return to operations. This phase includes compliance with other enterprise and facility practices and procedures including those specific to intelligent devices/IACS.

A.8.9 Decommissioning

A.8.9.1 General

In a digital world, decommissioning extends beyond removal of the physical device including the connections to the associated internal (device) and external (IACS plus) databases.

A.8.9.2 Archiving IDM data

Device removal includes the management of historical data generated by the device, maintenance of the archived data, which includes long term access, security, industry specific regulations, and associated costs.

A.8.9.3 Removal of devices

To avoid potential references to invalid or obsolete data, which could cause operational problems, all associated applications, databases, links and references using the intelligent device data are to be identified and cleaned up or set to a defined value representing invalid data.

A.8.9.4 Refurbishment (for return to inventory)

If returned to facility stores for reuse elsewhere in the facility, the intelligent device is overhauled to a defined base condition as this will ensure that when it is ready to be used in a different application, no residual information will affect the new use and that each new configuration starts from the same base case.

A.8.9.5 Disposal (non-salvage)

Intelligent devices that leave the facility with facility configuration data can release intellectual property.

A.9 Supplier requirements

A.9.1 Objective

The objective of Clause 9 is to provide guidance for developing supplier requirements for intelligent devices, systems, software and services and other supporting products that are part of an IDM program.

A.9.2 General

Owner operators work with intelligent device suppliers to support the development and implementation of an IDM program within the owner operator enterprise. Having a set of requirements, specifications, and work processes enables the relationship between owner operator and supplier to be effective throughout the IDM life cycle.

A.9.3 Products

A.9.3.1 Devices

Device requirements are necessary for establishing and maintaining device integrity while supporting integration with the IACS.

A.9.3.2 IACS

IACS requirements provide for proper support for IACS integration of devices and for long term support including device maintenance and replacement.

A.9.3.3 Software

Software requirements support supply chain integrity and revision or migration.

A.9.4 Services

A.9.4.1 Engineering/project support

If they have not done so already, suppliers of equipment, associated services, and engineering suppliers supporting the IDM program are encouraged to incorporate IDM practices in their traditional workflow and practices.

A.9.4.2 Operations and maintenance support

Although requiring input and development during the design phase, IDM has the largest impact during the operations life cycle phase and therefore ongoing support is critical to the success of the program. Support during this phase is often provided as a combination of site and remote (company/enterprise and third party) personnel. This is the reason a well-documented plan is required.

NOTE IDM also provides significant benefits during commissioning, which is another reason to include it as part of the development phase.

A.9.4.3 Personnel competency

Services are, by their nature, provided by people and therefore the individuals providing these services are expected to be competent and capable of completing the assigned tasks.

A.9.4.4 Cybersecurity

Automation and control systems are critical infrastructures for the safe and reliable operation of facilities and consequently can also have associated cybersecurity statutory requirements. IDM, which relies on configurable devices and digital communications that are important IACS elements, also needs to incorporate cybersecurity practices.

A.9.5 Device support tools

A variety of different hardware and software support equipment is required to communicate, modify, and maintain intelligent devices. This subclause provides guidance on their use.

A.10 Information management

A.10.1 Objective

Clause 10 provides information on the overall management of information identified in the other clauses in this document.

Information management best practices are applied to IDM information management.

A.10.2 General

Effective information management covers all parts of IDM life cycles (facility, product, etc. life cycles).

A.10.3 Information collection, exchange, reconciliation, and storage

This subclause identifies the best practice mechanisms for IDM information management. These include information quality, information collection validation and reconciliation. Cybersecurity, retention and storage including data access and management is also addressed.

These mechanisms are necessary to provide an effective and efficient management system for intelligent devices.

A.10.4 IDM information

The IDM program is most effective when the large amounts of disparate data types and sources are managed as a part of an integrated IDM system. The identification and inclusion of appropriate information types is necessary for effective IDM information management.

This subclause identifies the minimum data and information sources that form an IDM information management system.

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

Bibliography

- IEC 60793-1-40:2019, *Optical fibres – Part 1-40: Attenuation measurement methods*
- IEC 61158-4-2:2023, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*
- IEC 61400-22:2010², *Wind turbines – Part 22: Conformity testing and certification*
- IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*
- IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*
- IEC 61918, *Industrial communications networks – Installation of communication networks in industrial premises*
- ISO/IEC Directives Part 2:2021, *Principles and rules for the structure and drafting of ISO and IEC documents*
- ISO/IEC Guide 2:2004, *Standardization and related activities – General vocabulary*
- ISO/IEC TR 18053:2000, *Information technology – Telecommunications and information exchange between systems – Glossary of definitions and terminology for Computer Supported Telecommunications Applications (CSTA) Phase III*
- ISO/IEC 11179-6, *Information technology – Metadata registries (MDR) – Part 6: Registration*
- ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*
- ISO/IEC 30105-4:2016³, *Information technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes – Part 4: Terms and concepts*
- ISO 27914:2017, *Carbon dioxide capture, transportation and geological storage – Geological storage*
- ISO 28219:2017, *Packaging – Labelling and direct product marking with linear bar code and two-dimensional symbols*
- ISA5.1, *Instrumentation Symbols and Identification*
- ISA84, *Instrumented Systems to Achieve Functional Safety in the Process Industries*
- ISA TR84.00.09, *Cybersecurity Related to the Functional Safety Lifecycle*
- ISA99, *Industrial Automation and Control Systems Security*

² Withdrawn.

³ Withdrawn.

NAMUR NE 043, *Standardization of the Signal Level for the Failure Information of Digital Transmitters*

NAMUR NE 107, *Self-Monitoring and Diagnosis of Field Devices*

NFPA 70 Article 250 "*Grounding and Bonding*"

NIST 800 series, *Cybersecurity framework*

IECNORM.COM : Click to view the full PDF of IEC 63082-2:2024

SOMMAIRE

AVANT-PROPOS	107
INTRODUCTION.....	109
1 Domaine d'application	110
2 Références normatives	110
3 Termes, définitions, abréviations et conventions.....	111
3.1 Termes et définitions	111
3.2 Abréviations.....	112
3.3 Conventions.....	113
4 Exigences fondamentales applicables à la gestion des appareils intelligents	113
4.1 Objectif.....	113
4.2 Généralités	114
4.3 Fonctions de gestion.....	114
4.4 Processus et procédures de travail formels et informels.....	114
4.5 Gestion des modifications	115
4.5.1 Généralités	115
4.5.2 Évaluation d'impact	116
4.5.3 Planification.....	116
4.5.4 Formation	116
4.5.5 Documentation	116
4.5.6 Conservation des données et des documents	116
4.6 Gestion des risques	116
5 Gestion des risques	117
5.1 Objectif.....	117
5.2 Généralités	117
5.3 Exigences des programmes IDM.....	117
5.4 Coordination des programmes	118
5.5 Gestion des risques au niveau de l'installation.....	118
5.6 Gestion des risques liés aux fournisseurs	119
5.7 Risques liés à la gestion de l'information	120
5.8 Gestion des risques liés à la cybersécurité	120
6 Gestion au niveau de l'entreprise pour l'IDM.....	120
6.1 Objectif.....	120
6.2 Généralités	121
6.3 Organisation et ressources	121
6.4 Élaboration et maintien d'un programme IDM.....	122
6.5 Gestion des fournisseurs	123
6.5.1 Coordination avec les fournisseurs	123
6.5.2 Gestion du cycle de vie des appareils intelligents	123
6.5.3 Cycle de vie de la technologie des appareils	124
6.6 Élaboration et maintien des modèles de processus de travail IDM	124
6.7 Gestion et conception de programmes IDM.....	126
6.7.1 Gestion des ressources	126
6.7.2 Amélioration de la conception et des performances de programmes IDM.....	126
6.7.3 Retour d'information sur les performances des programmes IDM à la direction	126
6.7.4 Fonctionnement des programmes IDM.....	126

6.7.5	Soutien et suivi des programmes IDM pour les installations	127
7	Mise en œuvre d'une coordination entre l'entreprise, les installations et les fournisseurs.....	127
7.1	Objectif	127
7.2	Généralités	127
7.3	Mise en œuvre de l'IDM	127
7.3.1	Principes communs	127
7.3.2	Mise en œuvre de l'IDM dans les nouvelles installations.....	128
7.3.3	Mise en œuvre de l'IDM dans les installations existantes.....	129
7.3.4	Mise en œuvre des processus de travail IDM dans une installation.....	129
7.4	Coordination pour une amélioration continue	129
7.4.1	Généralités	129
7.4.2	Évaluation et audits des activités IDM.....	130
7.4.3	Résolution des causes de non-conformités des programmes	130
7.5	Coordination avec d'autres programmes d'entreprise	131
7.5.1	Généralités	131
7.5.2	Coordination du cycle de vie des activités de programme	131
7.5.3	Applications	131
7.5.4	Informations concernant l'appareil/processus	131
7.5.5	Systèmes, réseaux et sécurité	132
7.5.6	Phases du cycle de vie	132
7.5.7	Interfaces d'application pour la coordination	132
8	Phases du cycle de vie de l'installation.....	132
8.1	Objectif	132
8.2	Généralités	133
8.3	Gestion des phases du cycle de vie de l'installation	133
8.3.1	Généralités	133
8.3.2	Points d'entrée du cycle de vie	134
8.3.3	Modifications des installations	134
8.4	Élaboration du domaine d'application.....	134
8.4.1	Généralités	134
8.4.2	Objectif.....	136
8.4.3	Gestion des risques	136
8.4.4	Considérations relatives au type de projet	136
8.4.5	Planification et conception de la mise en œuvre de l'IDM	137
8.4.6	Définition de plans de soutien à long terme de l'installation	137
8.4.7	Plan de transfert à l'exploitation et à la maintenance	138
8.4.8	Définition d'une stratégie de cybersécurité pour les appareils intelligents.....	139
8.4.9	Choix de solutions alternatives de conception.....	140
8.4.10	Préparation des outils et de leurs procédures	141
8.4.11	Choix des fournisseurs	142
8.4.12	Planification de la gestion de l'information	143
8.5	Conception et ingénierie	144
8.5.1	Objectif.....	144
8.5.2	Généralités	144
8.5.3	Choix d'un appareil.....	145
8.5.4	Acquisition de l'appareil intelligent.....	147
8.5.5	Préparation des données de configuration	148

8.5.6	Mise en œuvre et intégration des fonctions des appareils intelligents avec l'IACS.....	153
8.5.7	Exigences en matière d'intégration et d'essai des systèmes	155
8.6	Construction et mise en service	156
8.6.1	Généralités	156
8.6.2	Mise en place du site	157
8.6.3	Installation	157
8.6.4	Approvisionnement	158
8.6.5	Configuration	158
8.6.6	Contrôle de boucle et mise en service	159
8.6.7	Formation et compétence du personnel	160
8.6.8	Transfert.....	161
8.6.9	PSSR	161
8.6.10	Démarrage	161
8.7	Exploitation et maintenance	162
8.7.1	Généralités	162
8.7.2	Processus de surveillance continue des appareils intelligents, et processus d'identification et de diagnostic des problèmes	162
8.7.3	Étalonnage des appareils intelligents.....	164
8.7.4	Processus de réparation	164
8.7.5	Remplacement des appareils intelligents.....	166
8.7.6	Gestion des stocks d'appareils intelligents.....	170
8.7.7	Processus de post-réparation	170
8.8	Révisions	172
8.8.1	Généralités	172
8.8.2	Préparation de la révision	172
8.8.3	Planification de révision.....	173
8.8.4	Exécution de la révision.....	173
8.8.5	Remise en service et démarrage	174
8.9	Démantèlement.....	174
8.9.1	Généralités.....	174
8.9.2	Archivage des données IDM	174
8.9.3	Retrait des appareils.....	174
8.9.4	Remise en état (pour retour en stock).....	175
8.9.5	Élimination (non récupérable)	175
9	Exigences relatives au fournisseur	175
9.1	Objectif	175
9.2	Généralités	175
9.3	Produits	175
9.3.1	Appareils	175
9.3.2	IACS.....	176
9.3.3	Logiciels	177
9.4	Services.....	178
9.4.1	Assistance ingénierie/projet.....	178
9.4.2	Soutien de l'exploitation et de la maintenance	178
9.4.3	Compétence du personnel	179
9.4.4	Cybersécurité	179
9.5	Outils de support des appareils.....	180
9.5.1	Modèles d'appareils intelligents	180

9.5.2	Outils IDM	180
9.5.3	Soutien à l'interopérabilité du système de gestion des appareils intelligents	180
9.5.4	Outils de migration, configuration et maintenance	180
10	Gestion de l'information	181
10.1	Objectif	181
10.2	Généralités	181
10.3	Collecte, échange, rapprochement et stockage des informations	182
10.3.1	Collecte et rapprochement	182
10.3.2	Cybersécurité	183
10.3.3	Procédures de stockage et de conservation des informations	183
10.3.4	Fonctions de gestion des données	184
10.4	Informations IDM	185
10.4.1	Généralités	185
10.4.2	Information: Dossiers de maintenance et de fiabilité	185
10.4.3	Information: Modèles et calculs	186
10.4.4	Information: Documents et schémas	186
10.4.5	Information: Identification des processus et procédures de travail	186
10.4.6	Information: Compétence en matière de rôle des travailleurs	186
10.4.7	Information: Configuration des appareils intelligents	186
10.4.8	Information: Outils	187
Annexe A (informative)	Notes explicatives des articles	188
A.4	Exigences fondamentales applicables à la gestion des appareils intelligents	188
A.4.1	Objectif	188
A.4.2	Généralités	188
A.4.3	Fonctions de gestion	188
A.4.4	Processus et procédures de travail formels et informels	188
A.4.5	Gestion des modifications	188
A.5	Gestion des risques	188
A.5.1	Objectif	188
A.5.2	Généralités	189
A.5.3	Exigences des programmes IDM	189
A.5.4	Coordination des programmes	189
A.5.5	Gestion des risques au niveau de l'installation	189
A.5.6	Gestion des risques liés aux fournisseurs	189
A.5.7	Risques liés à la gestion de l'information	189
A.5.8	Gestion des risques liés à la cybersécurité	189
A.6	Gestion au niveau de l'entreprise pour l'IDM	190
A.6.1	Objectif	190
A.6.2	Généralités	190
A.6.3	Organisation et ressources	190
A.6.4	Élaboration et maintien d'un programme IDM	191
A.6.5	Gestion des fournisseurs	191
A.6.6	Élaboration et maintien des modèles de processus de travail IDM	192
A.6.7	Gestion et conception de programmes IDM	192
A.7	Mise en œuvre d'une coordination entre l'entreprise, les installations et les fournisseurs	192
A.7.1	Objectif	192
A.7.2	Généralités	192

A.7.3	Mise en œuvre de l'IDM.....	193
A.7.4	Coordination pour une amélioration continue	193
A.7.5	Coordination avec d'autres programmes d'entreprise.....	194
A.8	Phases du cycle de vie de l'installation	195
A.8.1	Objectif.....	195
A.8.2	Généralités	195
A.8.3	Gestion des phases du cycle de vie de l'installation.....	195
A.8.4	Élaboration du domaine d'application	196
A.8.5	Conception et ingénierie	198
A.8.6	Construction et mise en service	200
A.8.7	Exploitation et maintenance	201
A.8.8	Révisions.....	204
A.8.9	Démantèlement	205
A.9	Exigences relatives au fournisseur.....	206
A.9.1	Objectif.....	206
A.9.2	Généralités	206
A.9.3	Produits	206
A.9.4	Services	206
A.9.5	Outils de support des appareils	207
A.10	Gestion de l'information	207
A.10.1	Objectif.....	207
A.10.2	Généralités	207
A.10.3	Collecte, échange, rapprochement et stockage des informations	207
A.10.4	Informations IDM	207
	Bibliographie.....	208
	Figure A.1 – Vue d'ensemble du processus de réparation de boucle.....	202
	Figure A.2 – Présentation de l'évaluation de la nouvelle conception des appareils intelligents et de leur remplacement.....	203
	Tableau A.1 – Documents d'orientation pour l'installation	200

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES APPAREILS INTELLIGENTS –

Partie 2: Exigences et recommandations

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments du présent document de l'IEC peuvent faire l'objet de droits de brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété. À la date de publication du présent document, l'IEC n'a reçu aucune déclaration relative à des droits de brevets, qui pourraient être exigés pour la mise en œuvre du présent document. Toutefois, il est rappelé aux responsables de cette mise en œuvre qu'il ne s'agit peut-être pas des informations les plus récentes, qui peuvent être obtenues dans la base de données disponible à l'adresse <https://patents.iec.ch>. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 63082-2 a été établie par le sous-comité 65E: Les dispositifs et leur intégration dans les systèmes de l'entreprise, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65E/1079/FDIS	65E/1112/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La version française de la norme n'a pas été soumise au vote.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Une liste de toutes les parties de la série IEC 63082, publiées sous le titre général *Gestion des appareils intelligents*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

INTRODUCTION

L'objectif de la série IEC 63082 est de définir un environnement qui permet l'utilisation efficace des appareils intelligents. La série IEC 63082 définit les concepts, la terminologie et les activités de gestion communs.

La gestion des appareils intelligents (IDM - *intelligent device management*) représente les activités de gestion des appareils intelligents tout au long du cycle de vie de l'installation et n'implique pas un outil particulier de gestion des actifs ou un ensemble de ces outils. Les outils matériels et logiciels sont nécessaires pour soutenir les processus et procédures de travail, mais la spécification des outils ne fait pas partie de la série IEC 63082. L'IDM est l'un des nombreux programmes d'entreprise. Les activités IDM optimisent la valeur des appareils intelligents et viennent à l'appui de l'intégration des données du niveau de la production aux systèmes d'entreprise. L'IDM est compatible avec les initiatives de fabrication intelligente.

Plusieurs parties prenantes sont responsables de la réussite de la gestion des appareils intelligents, notamment les prestataires de projets d'ingénierie, d'achat et de construction (EPC), les intégrateurs de systèmes, les fournisseurs et les consultants.

La série IEC 63082 n'est pas destinée à remplacer ou à contredire d'autres normes, par exemple la série IEC 61511 pour les systèmes instrumentés de sécurité et la série IEC 62443 pour la cybersécurité.

L'IEC TR 63082-1 définit les concepts et la terminologie de la gestion des appareils intelligents nécessaires à une compréhension approfondie et à une communication efficace. Elle présente les concepts de base du mode de gestion des appareils intelligents et donne un aperçu du fonctionnement de cette gestion tout au long du cycle de vie de l'installation. L'IEC TR 63082-1 fournit les connaissances de base pour comprendre les concepts de gestion des appareils intelligents nécessaires à la mise en œuvre d'un programme IDM.

Le présent document fournit des dispositions (exigences et recommandations). L'Annexe A informative fournit des informations supplémentaires concernant la raison pour laquelle des exigences sont spécifiées. Les informations fournies dans l'IEC TR 63082-1 sont destinées à servir de matériau de base pour une meilleure compréhension des dispositions du présent document.

GESTION DES APPAREILS INTELLIGENTS –

Partie 2: Exigences et recommandations

1 Domaine d'application

La présente partie de l'IEC 63082 spécifie les exigences et les recommandations qui permettent d'établir et de maintenir la gestion des appareils intelligents (IDM) telle que décrite dans l'IEC TR 63082-1 dans une entreprise qui comporte une ou plusieurs installations.

Les sujets suivants relèvent du domaine d'application du présent document:

- l'optimisation des fonctionnalités et des performances des appareils intelligents pour leur utilisation;
- la gestion des informations liées à l'IDM;
- l'intégration d'appareils intelligents dans les systèmes d'automatisation et de commande industrielles (IACS - *industrial automation and control systems*) des installations;
- l'échange d'informations entre les parties prenantes qui réalisent et maintiennent l'IDM;
- la coordination de plusieurs cycles de vie asynchrones de l'IDM.

Les sujets suivants ne relèvent pas du domaine d'application du présent document:

- la définition et la détermination de la fonction et des performances des appareils intelligents;
- la définition et la spécification des technologies et des outils qui fournissent, préservent et gèrent les informations liées à l'IDM, comme les outils FDT, FDI, outils portables en ligne et hors ligne, outils de configuration, historiques et outils de planification de la maintenance;
- la définition et la spécification des technologies et des outils de conception des appareils intelligents;
- la définition et la spécification de l'architecture des réseaux de communication, des technologies de communication, des exigences en matière de cybersécurité et des exigences en matière de gestion des réseaux.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62381, *Systèmes d'automatisation pour les procédés industriels – Essais d'acceptation en usine (FAT), essais d'acceptation sur site (SAT) et essais d'intégration sur site (SIT)*

IEC 62382, *Systèmes de commande pour les procédés industriels – Contrôle de boucle des circuits électriques et des appareillages.*

IEC 62443 (toutes les parties), *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*

IEC TR 63082-1:2020 *Intelligent device management – Part 1: Concepts and terminology* (disponible en anglais seulement)

3 Termes, définitions, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'IEC TR 63082-1 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <https://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>

3.1.1

certification

procédure par laquelle une tierce partie s'engage de manière documentée sur la conformité avec des exigences spécifiées d'un produit, d'un processus ou d'un service

[SOURCE: IEC 61400-22:2010, 3.4, modifié – "par écrit" a été remplacé par "de manière documentée" et "également appelée évaluation de la conformité" a été supprimé.]

3.1.2

démantèlement

acte de mettre un système ou un composant technique hors service, de le rendre inopérant, de le démonter et le décontaminer

[SOURCE: ISO 27914:2017, 3.13, modifié – "démanteler" a été remplacé par "démantèlement", et "mettre" a été remplacé par "acte de mettre".]

3.1.3

dispositif de surveillance d'appareil

fonctions et activités de suivi du comportement d'un appareil, et pour tous les appels associés à ce dernier

[SOURCE: ISO/IEC TR 18053:2000, 3.141, modifié – Le terme anglais "Device-Type Monitor" a été remplacé par le terme "device monitoring", l'expression française "moniteur qui suit" a été remplacée par "fonctions et activités de suivi", et l'expression française "fournissant des notifications d'événements pour l'appareil" a été supprimée.]

3.1.4

exigence fondamentale

exigence qui sert de base à la dérivation des exigences détaillées

EXEMPLE Gestion du risque, gestion de la fonctionnalité et des performances, gestion des modifications.

Note 1 à l'article: Il est possible que les exigences fondamentales ne soient pas directement applicables, mais il convient que les exigences qui en découlent servent de base à l'action.

3.1.5

organisation

organisme qui est fondé sur la participation ou l'adhésion d'autres organismes ou de particuliers et qui est doté de statuts bien établis et de sa propre administration

[SOURCE: Guide ISO/IEC 2:2004, 4.2]

3.1.6

exploitant direct

entreprise ou organisme responsable du fonctionnement quotidien d'une installation

Note 1 à l'article: L'exploitant direct peut déléguer contractuellement tout ou partie de ces responsabilités.

3.1.7

système de management de la qualité

SMQ

cadre organisationnel dont la structure fournit les politiques, processus, procédures et ressources exigés pour la mise en œuvre du plan de management de la qualité

Note 1 à l'article: Il convient que le plan type de management de la qualité d'un projet soit compatible avec le système de management de la qualité de l'organisation.

[SOURCE: ISO/IEC 30105-4:2016, 3.41, modifié – l'article anglais "the" a été supprimé.]

3.1.8

exigence

expression, dans le contenu d'un document, formulant les critères objectivement vérifiables à respecter et avec lesquels aucun écart n'est permis afin de prétendre à la conformité avec le document

Note 1 à l'article: Les exigences peuvent décrire un service, une capacité, une caractéristique ou une activité essentiels.

[SOURCE: Directives ISO/IEC Partie 2:2021, 3.3.3]

3.1.9

fournisseur

partie qui produit, fournit ou procure un article, un système ou un service

[SOURCE: ISO 28219:2017, 3.11, modifié – "système" a été ajouté.]

3.1.10

outil

logiciel exécutable qui interagit avec l'utilisateur pour exécuter une fonction donnée

EXEMPLE Logiciel de planification de liaison (LSS).

Note 1 à l'article: L'abréviation "LSS" est dérivée du terme anglais développé correspondant "link scheduling software".

[SOURCE: IEC 61158-4-2:2023, 3.4.73]

3.2 Abréviations

AVL	(approved vendor list) liste des fournisseurs agréés
DIN	(Deutsches Institut für Normung) Institut allemand de normalisation
DP	demande de proposition
DTM	(device type manager) gestionnaire type d'appareils
EAM	(enterprise asset maintenance) maintien des actifs d'entreprise
EDD	(electronic device description file) fichier de description d'appareil électronique
EPC	ingénierie, achat et construction
FAT	(factory acceptance test) essai de réception en usine
FDI	(field device Integration) intégration des appareils de terrain
FDT	(field device tool) outil des appareils de terrain

HAZOP	(hazard and operability study) étude des dangers et de l'exploitabilité
IACS	(industrial automation control system) système de contrôle-commande industriel
IAO	ingénierie assistée par ordinateur
IDM	(intelligent device management) gestion des appareils intelligents
IED	(intelligent electronic device) appareil électronique intelligent
IHM	interface homme machine
IPC	indicateur de performance clé
ISA	International Society of Automation
LOPA	(layer of protection analysis) analyse des couches de protection
MES	(manufacturing execution system) système d'exécution de fabrication
MOC	(management of change) gestion des modifications
MRO	(maintenance repair and operations) maintenance, réparation et exploitation
MTBF	moyenne des temps de bon fonctionnement
NAMUR	Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie
NEC	(national electrical code) Code national de l'électricité
NIST	(National Institute of Standards and Technology) institut national des normes et des technologies
OT	(operations technology) technologie d'exploitation
PAM	(plant asset management) gestion des actifs de l'installation
PRE	planification des ressources de l'entreprise
PSSR	(pre-start-up safety review) revue de sécurité avant démarrage
PV	process variable (variable de processus)
RAM	(responsibility assignment matrix) matrice d'attribution des responsabilités
SAT	(site acceptance test) essai de réception sur site
SIGE	système informatisé de gestion de la maintenance
SMQ	système de management de la qualité
SIT	(site integration test) essai d'intégration sur site

3.3 Conventions

Pour aider l'utilisateur du présent document à le comprendre sans exiger de se référer à l'IEC 63082-1, l'Annexe A contient des informations contextuelles pour chacun des titres des niveaux 1 à 3 du document principal.

4 Exigences fondamentales applicables à la gestion des appareils intelligents

4.1 Objectif

Le présent article spécifie les exigences fondamentales et les recommandations pour atteindre et maintenir l'IDM.

Les exigences fondamentales constituent la base des exigences détaillées ou dérivées dans le reste du présent document.

Les exigences et recommandations du présent article s'appliquent à tous les produits, services et activités liés à l'IDM et à sa gestion.

NOTE Les produits et les technologies associées comprennent, entre autres, les appareils intelligents et le matériel et les logiciels de l'IACS. Ces exigences fondamentales s'appliquent à tous les cycles de vie.

4.2 Généralités

La gestion des appareils intelligents doit être établie tant pour les nouvelles installations que pour les installations existantes.

Toutes les organisations impliquées dans la fourniture et la distribution d'appareils intelligents, les organisations qui fournissent des outils et des services à l'appui des appareils intelligents, et les organisations qui utilisent ou exploitent des installations employant des appareils intelligents doivent être considérées comme des participants au programme IDM.

L'IDM doit être maintenu et amélioré en permanence pour s'adapter aux modifications technologiques et organisationnelles.

Il convient de mettre en œuvre l'IDM de manière cohérente dans une entreprise qui comprend plusieurs installations.

NOTE L'IDM considère par hypothèse une certaine souplesse dans son mode de mise en œuvre pour répondre aux besoins des différentes installations d'une entreprise.

L'IDM doit couvrir l'intégration d'appareils dans l'IACS.

4.3 Fonctions de gestion

La gestion des appareils intelligents doit inclure les fonctions et les organisations nécessaires à la coordination d'autres programmes de gestion et des ressources organisationnelles internes et externes. Les organisations doivent assurer la disponibilité des ressources pour la mise en œuvre de l'IDM.

NOTE 1 L'un des principaux objectifs d'un programme IDM est la coordination avec d'autres programmes externes. Par exemple: Les programmes d'alliance avec les fournisseurs peuvent apporter une contribution et un soutien direct à l'IDM.

NOTE 2 Un programme est un moyen efficace et formel de gérer et de coordonner des activités telles que l'IDM.

L'IDM doit soutenir les programmes de gestion des risques en fournissant des données pour l'évaluation des risques associés, y compris ceux liés aux défaillances matérielles aléatoires, aux défaillances de cause commune (par exemple, configuration système, conception, installation, intégration et maintenance) et à la cybersécurité.

L'IDM doit être développé avec le parrainage, l'appropriation et la responsabilité de la direction.

Des procédures et des processus doivent être établis pour surveiller et mesurer les performances de l'IDM.

NOTE 3 Trois indicateurs de performances clés (IPC) constituent une technique courante de surveillance et de mesure des performances.

4.4 Processus et procédures de travail formels et informels

Les organisations qui comportent un programme IDM doivent décider si chacun de leurs processus de travail est un processus de travail formel ou informel. Chaque organisation qui participe à l'IDM doit définir les exigences de ces processus et procédures de travail.

Les processus et les procédures de travail, ainsi que les tâches nécessaires à la réalisation des exigences fondamentales doivent être définis:

- les activités à réaliser;
- les compétences et connaissances préalables; et
- un programme de formation pour permettre aux travailleurs de développer ces compétences et connaissances.

Les processus de travail incluent les sujets suivants:

- les exigences relatives aux processus et procédures de travail formels et informels;
- l'exigence d'un processus géré pour les décisions, facteurs; et
- les caractéristiques qui déterminent les processus de travail informels et formels.

NOTE 1 Les processus de travail formel et informel sont dérivés des exigences fondamentales.

NOTE 2 Les processus de travail formels comprennent les processus pour lesquels les écarts par rapport aux processus de travail et leurs produits livrables associés sont gérés conformément aux exigences de la MOC définies dans le programme IDM.

NOTE 3 Les processus de travail informels comprennent ceux qui sont acceptés comme partie intégrante de la formation de base pour un travail qualifié et englobent les bonnes pratiques courantes telles que l'entretien ménager.

Il convient de prendre la décision de rendre un processus de travail formel ou informel sur la base des critères suivants, entre autres:

- a) forte complexité;
- b) nombre de personnes ou d'organisations impliquées;
- c) transferts de propriété ou propriétaires multiples;
- d) niveaux de risques élevés;
- e) fréquence d'utilisation;
- f) besoin de stabilité, de reproductibilité et d'exactitude pendant de longues durées.

Il convient que les processus et procédures de travail formels incluent, entre autres:

- a) des conditions de départs ou des éléments d'entrée définis;
- b) des processus internes définis, y compris des rôles et responsabilités définis;
- c) des outils et une infrastructure définis;
- d) des ressources en personnel définies (nombre, identité et compétence);
- e) des interfaces externes définies;
- f) une réalisation et un résultat définis;
- g) un soutien financier, des mesures de réussite et une responsabilité de gestion définis;
- h) une documentation et une formation formelles.

Le programme IDM doit répondre aux exigences de sécurité des appareils intelligents et de cybersécurité des systèmes IACS.

NOTE 4 La sécurité des appareils intelligents est une condition dans laquelle les ressources du système sont protégées contre tout accès non autorisé et contre toute modification, destruction ou perte non autorisée ou accidentelle.

EXEMPLE La série IEC 62443 spécifie des exigences de cybersécurité pour les systèmes IACS.

4.5 Gestion des modifications

4.5.1 Généralités

Une gestion des modifications (MOC) doit être appliquée à tous les appareils, systèmes, outils, processus de travail, informations et ressources nécessaires à l'IDM.

NOTE 1 Les changements IDM comprennent, entre autres, les changements introduits par les fournisseurs d'appareils intelligents, tels que les modifications de révision ou les évolutions technologiques, les modifications de programme, d'outils ou de procédures IDM et les changements de personnel avec une responsabilité IDM.

NOTE 2 La MOC inclut la gestion de configuration telle que décrite au 8.6.5.

L'IDM doit prévoir la MOC à tous les niveaux ou sous-niveaux de l'organisation de l'entreprise.

Les rôles et responsabilités du personnel doivent être définis dans le programme IDM pour la gestion, l'exécution, le maintien et la documentation des modifications apportées aux appareils intelligents et aux systèmes IACS liés auxdits appareils.

4.5.2 Évaluation d'impact

Aucune activité de modification ne doit commencer avant qu'une évaluation d'impact ne soit réalisée et approuvée conformément aux procédures IDM.

L'évaluation d'impact doit prendre en considération l'impact à court et à long termes de la modification proposée. Si l'évaluation d'impact indique que la modification proposée a un impact négatif sur les exigences fonctionnelles, cet impact doit être résolu avant la mise en œuvre.

NOTE Étant donné qu'il est facile de modifier les configurations des appareils intelligents, il est important que seules les modifications qui ont satisfait à l'évaluation des incidences et au processus MOC soient mises en œuvre.

4.5.3 Planification

La planification de la modification et de la nouvelle vérification ultérieure doit être documentée et distribuée à tous les participants, y compris la réévaluation de l'impact des changements.

NOTE La planification des changements peut varier en fonction de la complexité et de l'impact des changements.

Les modifications et les nouvelles vérifications doivent être effectuées conformément au plan de modification approuvé.

4.5.4 Formation

Le personnel concerné doit être formé aux pratiques liées aux modifications des appareils intelligents avant la mise en œuvre de ces modifications.

4.5.5 Documentation

Toute la documentation affectée par les changements (y compris les procédures d'essai et d'acceptation) doit être mise à jour comme l'exige le programme IDM.

4.5.6 Conservation des données et des documents

La fonctionnalité spécifiée du système doit être conservée ou atteinte lorsque des changements sont apportés qui influent sur tout appareil intelligent ou composant connecté du système IACS.

Les documents historiques relatifs aux changements doivent être conservés comme cela est défini par le programme IDM.

Les sauvegardes des configurations des appareils intelligents et des informations des systèmes IACS connectés auxdits appareils doivent être conservées comme cela est spécifié par le programme IDM.

4.6 Gestion des risques

Les risques liés à l'IDM doivent être inclus dans la stratégie globale de gestion des risques de l'entreprise.

Le processus de gestion des risques de l'IDM doit être un processus systématique défini de façon formelle.

5 Gestion des risques

5.1 Objectif

Le processus de gestion des risques de l'IDM comprend l'identification de toutes les menaces potentielles qui peuvent survenir lors de la mise en œuvre de toute phase IDM. Le présent article identifie les processus de travail complémentaires qu'exige une entreprise pour éliminer, réduire le plus possible ou contrôler les risques potentiels associés à l'IDM.

Il convient de satisfaire à toutes les dispositions prévues dans le présent document pour éviter tout risque non géré.

Le présent article énumère les dispositions de gestion des risques dans l'ensemble du document, qui sont propres à l'IDM tout au long du cycle de vie.

5.2 Généralités

La gestion des risques de l'IDM doit identifier le processus global de mise en œuvre des exigences relatives à l'IDM comme cela est défini par l'entreprise.

Il convient d'intégrer les processus de travail pour le classement par criticité des appareils intelligents aux pratiques de gestion des risques existantes de l'entreprise comme cela est documenté dans le programme IDM.

L'IDM doit comporter des mécanismes d'atténuation des risques associés aux défaillances systématiques et aléatoires, aux défaillances de cause commune, aux menaces pour la cybersécurité, aux incidences financières et aux autres risques identifiés.

5.3 Exigences des programmes IDM

Le programme IDM doit comporter des processus de travail et des systèmes de gestion définis pour contrôler son efficacité en permanence.

Les programmes IDM doivent identifier la responsabilité des résultats de la gestion des risques.

Le programme IDM doit définir des mesures proactives de maintien de l'intégrité des programmes.

NOTE 1 Les mesures proactives peuvent inclure un personnel, un budget, des outils et une formation, ainsi que d'autres activités associées à la gestion des risques systématiques.

La gestion des risques de l'entreprise prévoit l'alignement des stratégies et des processus afin de gérer les objectifs et priorités concurrents associés aux activités à long terme de l'entreprise.

NOTE 2 Les objectifs et priorités concurrents peuvent inclure les dépenses en capital, la planification des ressources, les activités de maintenance, le calendrier de production et d'autres activités connexes.

La gestion des risques de l'IDM doit identifier et évaluer les risques potentiels pour tous les composants, systèmes, processus et outils de travail

NOTE 3 Chaque entreprise détermine le processus d'évaluation à employer.

NOTE 4 Les risques potentiels peuvent inclure des risques pour l'installation, les fournisseurs et l'intégrité de l'approvisionnement, les buts et objectifs de l'entreprise et d'autres facteurs.

5.4 Coordination des programmes

La gestion des risques de l'IDM doit être coordonnée avec les autres programmes de gestion des risques au niveau de l'entreprise et au niveau de l'installation.

NOTE 1 La gestion des risques de l'IDM n'est pas indépendante des programmes de gestion des risques au niveau de l'entreprise et au niveau de l'installation.

NOTE 2 La coordination des programmes est une activité centrale de la gestion des risques.

NOTE 3 L'appréciation du risque constitue une composante de la gestion globale des risques de l'entreprise et la définition des exigences relatives à l'appréciation du risque ne relève pas du domaine d'application de l'IDM.

L'IDM doit s'aligner sur toutes les exigences des processus de travail de la stratégie de gestion des risques de l'entreprise.

Le processus de gestion des risques de l'IDM doit prévoir la mise en œuvre de stratégies de gestion des risques internes et externes.

NOTE 4 Les processus de gestion des risques internes et externes permettent de réduire la sévérité et/ou la probabilité d'un risque.

NOTE 5 Les stratégies de gestion des risques internes et externes peuvent inclure la coordination entre la production et la maintenance, les systèmes de transport, les fournisseurs, les événements non planifiés et d'autres considérations.

Le processus de gestion des risques de l'entreprise doit utiliser l'infrastructure de gestion des risques de cette dernière pour gérer les risques associés aux activités IDM.

NOTE 6 Le processus de gestion des risques de l'entreprise peut être l'analyse des couches de protection (LOPA), l'étude des dangers et de l'exploitabilité (HAZOP), la matrice de l'Institut allemand de normalisation (DIN: Deutsches Institut für Normung), la gestion des risques qualitative (QRA - *qualitative risk management*), l'analyse par arbre de panne et d'autres programmes définis.

5.5 Gestion des risques au niveau de l'installation

La gestion des risques doit commencer au début du cycle de vie de l'installation et se poursuivre tout au long de ce cycle.

NOTE 1 L'identification et la gestion des risques au début du cycle de vie de l'installation améliorent l'efficacité et l'efficacité de la gestion des risques pendant le reste du cycle de vie de l'installation.

Le programme IDM doit assurer la réalisation d'une évaluation de tous les déclencheurs de risques identifiés au cours du processus d'analyse des risques associé à l'IDM.

Les installations doivent utiliser un système de gestion du cycle de vie adapté à leurs exigences particulières, qui permet d'organiser un grand nombre d'activités séquentielles et parallèles interdépendantes afin de gérer les risques associés à ces activités.

NOTE 2 Le modèle de cycle de vie générique défini au 7.5 fournit un exemple des processus et procédures de travail pour les activités séquentielles et parallèles de gestion des risques de l'installation.

NOTE 3 Les activités séquentielles et parallèles peuvent être définies dans des organigrammes, des graphiques, des tableaux et d'autres représentations.

Le programme IDM doit permettre de gérer les déclencheurs d'événements initiaux (tels que les défaillances matérielles aléatoires), les conditions préalables, les effets en cascade et les contributions systématiques (telles que les procédures, le manque de ressources ou une formation inadéquate).

Le système de gestion du cycle de vie IDM doit intégrer des mesures de gestion des risques pour gérer les discontinuités entre les phases du cycle de vie.

NOTE 4 Les différentes phases du cycle de vie comprennent des changements de personnel, de rôles et de responsabilités, d'outils et de l'objectif principal des activités. Les transferts peuvent être perturbateurs s'ils ne sont pas gérés de manière correcte.

Les changements apportés à la fin d'un cycle de vie, y compris les activités hors séquence, doivent être gérés par le biais d'une MOC appropriée et recyclés par toutes les activités appropriées du cycle de vie.

NOTE 5 Les activités hors séquence (telles que la reprise) rompent les dépendances qui affectent le travail précédemment achevé.

NOTE 6 La détermination des points d'entrée appropriés du cycle de vie assure la réalisation des activités de recyclage nécessaires (voir 8.3).

Chaque phase du cycle de vie doit comporter des mécanismes de surveillance et d'audit pour assurer la gestion des risques.

Une documentation type doit être élaborée pour toutes les composantes du programme IDM.

NOTE 7 La documentation type peut inclure l'utilisation de modèles et d'outils (voir l'Article 10 pour la gestion de l'information).

La gestion des risques liés au cycle de vie doit comprendre, au minimum, les risques associés aux éléments suivants:

- a) données de configuration pour chaque appareil intelligent et ses systèmes hôtes:
 - 1) utilisation de modèles et d'outils types pour les appareils intelligents,
 - 2) paramètres à surveiller et à contrôler,
 - 3) réponse opportune et/ou exécution d'actions correctives pour les éléments suivants:
 - i) conditions de diagnostic,
 - ii) défaillances,
 - iii) performances dégradées ou anormales,
 - iv) questions de sécurité et d'accès,
 - v) non-conformité aux normes, règlements ou exigences;
- b) stratégie et planification de l'exploitation et de la maintenance:
 - 1) besoins en main-d'œuvre,
 - 2) calendrier,
 - 3) qualifications et formation,
 - 4) nombre de travailleurs qualifiés,
 - 5) fréquence des essais et examens;
- c) stratégie en matière de pièces de rechange:
 - 1) quantités,
 - 2) emplacements.

5.6 Gestion des risques liés aux fournisseurs

L'exploitant direct doit exiger des fournisseurs qu'ils gèrent les risques associés aux cycles de vie des produits et services.

NOTE 1 Les risques comprennent, entre autres, l'obsolescence et les mises à niveau des produits, les changements associés aux révisions des micrologiciels et des logiciels (se reporter à l'Article 9 pour les exigences relatives aux fournisseurs).

L'exploitant direct doit exiger des fournisseurs qu'ils coordonnent la gestion des risques liés aux produits et aux services avec les programmes de l'entreprise et avec les installations.

NOTE 2 Les fournisseurs et les installations travaillent ensemble pour gérer les changements (se reporter au 4.5).

5.7 Risques liés à la gestion de l'information

La gestion de l'information doit gérer les risques associés aux ensembles d'informations incomplets.

Elle doit également gérer les risques associés aux erreurs et aux divergences dans les informations qui proviennent de sources diverses.

NOTE 1 Des exemples de sources diverses peuvent inclure la documentation interne, la documentation externe et d'autres données sources telles que des manuels, des catalogues techniques.

La gestion de l'information doit gérer les risques associés aux changements observés au niveau des systèmes, des outils, du personnel et des procédures de gestion de l'information.

NOTE 2 Un exemple de changements d'information dans les projets comprend les changements entre la conception et l'exécution.

NOTE 3 Par exemple, les changements de personnel lors du transfert de l'équipe de projet vers une installation et les changements de personnel lors du changement d'équipe (voir 10.4).

5.8 Gestion des risques liés à la cybersécurité

Conformément aux principes de cybersécurité, l'accès à un système IACS doit être associé à des rôles au sein du système et des appareils bien définis et gérés de manière à assurer une fonctionnalité minimale pour accomplir les tâches exigées.

L'intégrité des données IDM doit être maintenue.

L'isolation entre les différents éléments du système IACS, y compris l'IDM, doit être conforme aux exigences de la série IEC 62443 relatives aux zones et au système de conduits/défense en profondeur.

L'accès et la gestion sécurisés des appareils doivent faire partie des pratiques de mise en œuvre de la cybersécurité d'une installation.

6 Gestion au niveau de l'entreprise pour l'IDM

6.1 Objectif

Le présent article spécifie des exigences et des recommandations pour l'élaboration, la maintenance et l'amélioration de la gestion au niveau de l'entreprise pour l'IDM.

La gestion IDM au niveau de l'entreprise inclut entre autres:

- a) un programme IDM qui comprend toutes les activités de gestion;
- b) l'infrastructure, y compris les systèmes hôtes;
- c) les ressources, y compris les compétences et le budget;
- d) la planification et la coordination de cycles de vie multiples, notamment le cycle de vie du programme IDM, les cycles de vie de la technologie des appareils, les cycles de vie des appareils, les cycles de vie des installations;

- e) la coordination entre les installations;
- f) des modèles de processus de travail.

NOTE Les modèles définissent les éléments de chaque processus de travail IDM dans un but spécifique commun à de nombreuses installations de l'entreprise. Ces modèles servent de base de mise en œuvre des processus de travail IDM dans une installation spécifique.

6.2 Généralités

Il convient que le programme IDM s'applique à toutes les installations de l'entreprise.

NOTE 1 Les installations ne sont pas toutes équipées d'appareils intelligents, et n'exigent donc pas d'IDM.

NOTE 2 La mise en œuvre de l'IDM peut s'effectuer progressivement dans plusieurs installations.

Les buts et objectifs de l'IDM doivent être pleinement documentés dans le programme IDM.

Ce programme doit être communiqué aux personnes et organisations responsables ayant un ou plusieurs rôles IDM.

NOTE 3 L'aptitude IDM peut être maintenue au moyen des outils, des compétences et des procédures qui peuvent être gérés de manière centralisée ou par l'intermédiaire des processus de travail répartis.

Des ressources compétentes pour la mise en œuvre et l'exécution de la gestion de configuration de l'IDM doivent être fournies pour effectuer les tâches exigées dans le délai défini.

Les critères de compétence doivent être établis par le programme IDM.

6.3 Organisation et ressources

La direction doit fournir toutes les ressources nécessaires pour réaliser et maintenir le programme IDM.

Elle doit spécifier le déploiement des ressources (ou la structure organisationnelle), y compris la consignation des relations et de l'emplacement.

Le programme IDM doit être communiqué aux organisations responsables.

NOTE 1 Les ressources peuvent être situées à distance de l'installation, peuvent être partagées par plusieurs installations, et peuvent être proposées par un fournisseur ou un entrepreneur.

L'entreprise doit identifier et documenter les rôles ayant l'autorité et la responsabilité d'assurer la réalisation et le maintien des objectifs de fonctionnalité et de performances pour l'IDM.

Les ressources impliquées dans l'IDM, comme le personnel et les outils, doivent être gérées afin qu'elles puissent être utilisées efficacement.

Des procédures (y compris la formation) doivent être mises en place pour gérer les compétences de toutes les personnes impliquées dans l'exécution d'un ou plusieurs rôles du programme IDM. Des évaluations des qualifications et compétences doivent être effectuées pour documenter la qualification des individus par rapport aux activités qu'ils accomplissent. Les individus qualifiés pour les rôles et les changements de personne dans un rôle doivent être documentés.

Chaque participant à l'IDM doit disposer de l'autorité et des ressources nécessaires pour remplir ses rôles et responsabilités.

Il convient que les programmes d'entreprise prévoient des processus de partage des solutions techniques et de gestion entre les différentes organisations qui couvrent les fournisseurs et les installations.

NOTE 2 Les solutions techniques et de gestion comprennent des outils et des modèles, des processus de travail et des procédures pour la gestion de la fonctionnalité et des performances.

Une procédure formelle doit être définie pour le remplacement du propriétaire d'un processus de travail IDM.

6.4 Élaboration et maintien d'un programme IDM

Un programme IDM doit être établi et documenté pour gérer les activités et l'infrastructure à long terme afin de résoudre les objectifs concurrents et de gérer leurs priorités.

Le statut de propriétaire d'un processus de travail IDM doit être attribué à une personne individuelle ou à un rôle.

Le remplacement du propriétaire d'un processus de travail IDM doit prendre en considération la planification de la succession et suivre la procédure définie correspondante.

Il convient d'établir le programme IDM en prenant en considération les sujets suivants:

- programmes de gestion des risques de l'entreprise;
- disponibilité des ressources;
- programmes d'assurance qualité;
- programme de sécurité;
- programme de sûreté;
- programme de gestion des actifs de l'entreprise.

Le programme IDM doit présenter une structure fonctionnelle bien définie.

NOTE 1 Un programme IDM peut prévoir l'organisation des fonctions de systèmes de gestion y compris MOC (voir 4.5).

Le programme IDM doit être défini de manière à ce que toutes les activités des différentes parties prenantes impliquées dans l'IDM d'une entreprise puissent être coordonnées efficacement.

Le programme IDM doit coordonner plusieurs cycles de vie asynchrones, y compris l'installation, les appareils, la technologie et les cycles de vie d'activité, ainsi que les processus de travail associés.

NOTE 2 L'IDM comporte certains processus de travail et dépend également de processus de travail qui ne relèvent pas de son domaine d'application.

NOTE 3 L'IDM peut être établie à toute phase du cycle de vie d'une entreprise ou d'une installation et peut inclure plusieurs installations actuelles et/ou futures, chacune à différentes phases du cycle de vie de l'IDM.

Le programme IDM doit être défini par un ensemble de buts, de stratégies et d'objectifs de gestion documentés.

L'efficacité du programme IDM doit être contrôlée et améliorée en permanence.

Le programme IDM doit être défini de manière à assurer les ressources et la responsabilité exigées.

Le programme IDM doit définir les rôles et les responsabilités exigés pour l'IDM. Ces rôles et responsabilités doivent être attribués au personnel et/ou aux organisations qualifiés.

La compétence exigée de chacun des rôles et des responsabilités associées doit être définie de manière à assurer la mise en œuvre appropriée de l'IDM.

Des programmes de formation doivent être définis pour assurer la compétence du personnel pour les rôles et les responsabilités associées pour soutenir le programme IDM.

NOTE 4 Les programmes de formation comprennent généralement, entre autres, une formation sur le matériel, les logiciels et les procédures associés.

La formation exigée pour soutenir le programme IDM et les dossiers d'évaluation des compétences doivent être identifiés et documentés à l'aide des outils désignés par l'installation.

NOTE 5 Les dossiers d'évaluation peuvent être conservés conformément aux politiques du propriétaire.

6.5 Gestion des fournisseurs

6.5.1 Coordination avec les fournisseurs

Un ensemble stable (à long terme) de fournisseurs compétents doit être établi pour les biens et les services qui correspondent aux équipements et aux technologies utilisés dans les installations.

NOTE 1 L'absence de stabilité fait peser sur la réingénierie une charge de gestion des changements et un risque excessif. Un changement de fournisseur peut exiger un effort important de réingénierie/configuration manuelle, ce qui est source d'erreurs et introduit un risque pour le projet.

NOTE 2 La stabilité permet également de prendre en charge l'intégration avec le reste des systèmes de l'entreprise, y compris les systèmes commerciaux, tout en permettant l'interopérabilité entre les systèmes hôtes et les appareils de terrain.

NOTE 3 L'une des formes de cette relation est l'alliance stratégique avec un fournisseur, par opposition à un processus d'appel d'offres ouvert pour chaque cycle d'acquisition de projet.

La gestion des fournisseurs doit s'effectuer sur la base d'un processus de travail documenté qui est régulièrement examiné, maintenu et mis à jour.

NOTE 4 Les fournisseurs changent au cours de la vie de l'installation.

NOTE 5 Les cycles de vie des installations, des appareils et des technologies ne sont pas synchronisés.

6.5.2 Gestion du cycle de vie des appareils intelligents

Un moyen de gérer les changements dans le cycle de vie des appareils doit être prévu.

Un processus/plan de soutien à la migration des produits doit être prévu.

Les changements dans le cycle de vie d'un appareil doivent être planifiés de manière à réduire le plus possible les perturbations de la fonctionnalité ou des performances dudit appareil.

NOTE 1 Il est possible que les changements dans le cycle de vie de l'appareil utilisent la même technologie, mais avec des modifications telles qu'une révision du logiciel qui force un changement dans la configuration de l'appareil.

La planification et le soutien technique doivent être complets et documentés avant la mise en œuvre des changements dans le cycle de vie de l'appareil.

NOTE 2 Les changements dans le cycle de vie des appareils peuvent souvent survenir à des moments autres que lors des arrêts de fonctionnement de l'usine ou d'autres modifications des installations.

Le programme IDM doit exiger des fournisseurs d'appareils qu'ils communiquent les informations nécessaires à la migration de la configuration entre les révisions successives des appareils.

NOTE 3 Voir également l'Article 9.

Les changements inattendus dans le cycle de vie de l'appareil constatés au moment de l'installation sont considérés comme des échecs de la MOC. Il convient d'étudier les échecs de la MOC dans le cycle de vie des appareils pour en éliminer les causes.

Des processus de travail doivent être établis pour assurer le maintien de l'intégrité de la conception tout au long du cycle de vie de l'appareil intelligent.

NOTE 4 L'intégrité de la conception exige de vérifier et de résoudre périodiquement les divergences entre la configuration telle qu'elle a été conçue et la configuration active (en cours d'exécution).

6.5.3 Cycle de vie de la technologie des appareils

Un moyen de gérer les évolutions technologiques pour les appareils intelligents doit être fourni.

NOTE 1 La gestion des évolutions technologiques comprend la planification qui vise à réduire le plus possible les perturbations.

NOTE 2 Une partie de la planification de la gestion des technologies, y compris la planification de l'obsolescence, peut être partagée avec les fournisseurs de technologies.

NOTE 3 Les évolutions technologiques peuvent être perturbatrices en raison du défaut d'interopérabilité et de l'incompatibilité avec les systèmes hôtes.

NOTE 4 Le défaut d'interopérabilité avec les systèmes hôtes peut exiger des plans d'amélioration des immobilisations à long terme.

Il convient d'éviter l'obsolescence technologique non gérée, qui constitue un échec de la MOC.

Les échecs technologiques de la MOC doivent être étudiés pour en éliminer les causes.

NOTE 5 Les évolutions technologiques peuvent entraîner des perturbations de l'approvisionnement en appareils.

Chaque technologie liée aux appareils intelligents doit être évaluée avec soin avant son déploiement. Cette évaluation doit inclure, au minimum, les éléments suivants:

- a) la maturité et la disponibilité des technologies (y compris la disponibilité à long terme);
- b) les sources d'approvisionnement et de soutien, y compris la qualité et la compétence;
- c) les certifications et homologations.

Le soutien technique doit être complet et documenté avant la mise en œuvre des évolutions technologiques.

NOTE 6 L'évolution technologique d'un appareil désigne une évolution de la technologie de communication ou de détection (par exemple, passage des ultrasons à un flux tourbillonnaire ou inversement), qui est distincte des évolutions dans le cycle de vie de la technologie.

6.6 Élaboration et maintien des modèles de processus de travail IDM

Il convient d'utiliser des modèles de processus de travail pour l'IDM.

Lorsque des modèles de processus de travail sont utilisés, ils doivent être définis et documentés avec un contenu minimal. Un modèle de processus de travail doit être défini de manière générique, indépendamment de la mise en œuvre, en prenant en considération les exigences et les recommandations spécifiées qui correspondent à la phase du cycle de vie de l'installation décrite à l'Article 8.

Les interactions entre les procédures de chaque processus de travail IDM doivent être spécifiées.

NOTE 1 Des graphiques d'activités à couloirs peuvent être utilisés pour spécifier les interactions.

Les modèles de processus de travail doivent être maintenus et améliorés en permanence.

Lorsqu'un modèle de processus de travail IDM est défini, les informations communes à plusieurs installations de l'entreprise doivent être incluses.

NOTE 2 Cette disposition rend les modèles de processus de travail IDM communs à plusieurs installations d'une entreprise.

Chaque modèle de processus de travail IDM doit identifier les dispositions facultatives et obligatoires pour la mise en œuvre.

Les modèles de processus de travail IDM doivent être définis de manière à inclure des options pour l'assistance locale et à distance.

NOTE 3 Le contenu des modèles de processus de travail IDM est différent selon la répartition des responsabilités entre les installations locales et l'assistance à distance

Un modèle de processus de travail doit inclure les éléments suivants:

- objectif;
- éléments d'entrée et de sortie;
- temps de démarrage;
- procédures;
- installation cible;
- propriétaire (selon le rôle);
- rôles et responsabilités types.

NOTE 4 Les éléments d'entrée et de sortie rendent claires les interactions entre les processus de travail IDM, puisque certains des éléments d'entrée sont des éléments de sortie d'autres processus de travail IDM.

NOTE 5 Le temps de démarrage indique le moment de déclenchement du processus de travail IDM.

Le programme IDM doit définir et développer des modèles d'appareils intelligents pour gérer les données de manière structurée et uniforme.

Le modèle d'appareil intelligent comporte généralement au minimum les informations suivantes:

- a) le numéro d'étiquette (le numéro d'étiquette est associé à l'application de l'appareil), la marque et le numéro de modèle;
- b) l'année de fabrication et le numéro de série (ces éléments permettent le suivi historique de l'appareil physique);
- c) le matériau de construction;
- d) la plage étalonnée/de l'instrument et les paramètres de défaillance (le cas échéant);
- e) le signal d'entrée/sortie;
- f) l'alimentation de l'appareil et les spécifications de câblage (par exemple, courant alternatif/continu, 2 fils/4 fils);
- g) tous les autres paramètres de configuration.

NOTE 6 Certains appareils comportent des informations supplémentaires comme le point de consigne, la pression de conception, la plage de fonctionnement, l'adresse de communication par défaut, etc.

Autant de modèles que nécessaire doivent être élaborés pour chaque révision d'un type d'appareil.

NOTE 7 Un modèle pour chaque type d'application classique de l'appareil est généralement suffisant.

NOTE 8 Les modèles sont généralement développés, entretenus et transmis par les fournisseurs.

6.7 Gestion et conception de programmes IDM

6.7.1 Gestion des ressources

Le programme IDM doit permettre d'orienter et de contribuer aux décisions de l'entreprise en matière de gestion des ressources, notamment en ce qui concerne le personnel, les investissements dans les outils de soutien et le budget.

6.7.2 Amélioration de la conception et des performances de programmes IDM

Le programme IDM doit assurer que les lignes directrices générales ou les modèles de programmes IDM sont adaptés à l'organisation de l'entreprise.

NOTE La conception du programme peut inclure l'élaboration de processus de travail internes et la formation et les outils associés, ainsi que l'élaboration du soutien de la part des fournisseurs.

Le ou les plans d'amélioration des performances doivent comporter des méthodes et des critères de collecte de données systématiques qui permettent d'identifier les questions/problèmes et de définir les actions correctives appropriées.

Les plans d'amélioration des performances peuvent inclure des audits ou des évaluations de programmes.

6.7.3 Retour d'information sur les performances des programmes IDM à la direction

Les programmes IDM doivent fournir des mesures pour suivre les performances du programme global et des installations qui mettent en œuvre le programme.

NOTE L'objectif du suivi des performances est de fournir des processus de retour d'information formels pour évaluer l'efficacité globale des différents éléments du programme IDM.

Le retour d'information sur les performances doit être utilisé pour développer des améliorations du processus et/ou des outils de travail afin de réduire le plus possible les insuffisances mesurées.

6.7.4 Fonctionnement des programmes IDM

Les programmes IDM doivent affecter des ressources destinées à traiter les éléments suivants:

- changements dans le modèle d'activité de l'entreprise;
- changements au niveau du personnel (comme les départs à la retraite);
- changements en matière de technologie;
- changements au niveau des fournisseurs;
- insuffisances identifiées au niveau des performances du programme.

NOTE Le fonctionnement d'un programme implique un travail d'élaboration continue qui exige des ressources pour la durée de vie du programme.

6.7.5 Soutien et suivi des programmes IDM pour les installations

Les programmes IDM doivent fournir un soutien à l'IDM dans les installations pour toutes les phases du cycle de vie desdites installations.

NOTE Ce soutien peut inclure la documentation, les modèles de processus de travail, la formation, le soutien technologique et l'assistance aux relations avec les fournisseurs, et toute autre ressource généralement exigée par les autres installations d'une entreprise.

7 Mise en œuvre d'une coordination entre l'entreprise, les installations et les fournisseurs

7.1 Objectif

Le présent article spécifie les exigences et les recommandations pour la coordination entre les participants impliqués dans le programme IDM, y compris l'entreprise, ses installations et d'autres parties prenantes telles que les fournisseurs d'appareils intelligents.

La coordination comprend entre autres:

a) le flux d'informations entre les participants au programme;

NOTE Les exemples d'informations comprennent, entre autres, les modèles d'appareils et de processus de travail, la résolution de problèmes et l'expérience (IPC).

b) le suivi et l'amélioration du programme IDM;

c) la mise en œuvre de l'IDM dans les installations;

d) la coordination des fournisseurs;

e) le suivi et la coordination des activités IDM dans/entre les installations.

7.2 Généralités

Les entreprises doivent définir des limites et établir des processus de coordination pour la coopération entre le programme IDM et les autres programmes de l'entreprise, si nécessaire.

7.3 Mise en œuvre de l'IDM

7.3.1 Principes communs

Les entreprises doivent mettre en œuvre des processus de coordination communs à plusieurs installations pour l'élaboration, la révision, la maintenance et l'amélioration du programme IDM.

Il convient que les installations établissent une coordination avec les fournisseurs, le programme IDM de l'entreprise et d'autres programmes. Les entreprises doivent mettre en œuvre des mécanismes d'amélioration continue du programme IDM, y compris des audits.

Elles doivent fournir des mesures de performances et des incitations pour le programme IDM.

Il convient d'adapter la mise en œuvre de l'IDM à chaque installation selon sa nature.

La date d'entrée en vigueur de la mise en œuvre du programme doit être documentée afin d'étayer les audits périodiques prévus par le plan qualité.

NOTE 1 En général, il s'agit de la date de mise en œuvre du programme IDM.

Chaque installation doit mettre en place une coordination entre les disciplines (électricité, planification, processus, opérations, etc.).

NOTE 2 Cette coordination peut exiger la modification des processus de travail existants.

L'IDM doit être mise en œuvre dans les installations conformément aux exigences et aux objectifs du programme IDM de l'entreprise à laquelle l'installation appartient.

L'infrastructure de base pour l'IDM doit être fournie pour chaque installation.

NOTE 3 L'infrastructure comprend les outils (c'est-à-dire le matériel, les logiciels) ainsi que les ressources organisationnelles et humaines.

NOTE 4 Les éléments communs du programme sont généralement disponibles sous forme d'une série d'options.

Le partage d'informations (problèmes, opportunités, solutions) entre les installations et les fournisseurs doit être mis en œuvre.

7.3.2 Mise en œuvre de l'IDM dans les nouvelles installations

Il convient de prévoir des processus de coordination pour la mise en œuvre et l'utilisation des outils de support IDM, ainsi que pour l'élaboration et la mise à jour des procédures relatives à ces outils, afin que les outils de support soient utilisés de manière correcte et mis en œuvre de façon cohérente dans plusieurs installations.

NOTE L'introduction de nouveaux outils et procédures de support IDM dans une installation est une activité à haut risque.

Il convient que les processus de coordination traitent des sujets suivants, y compris:

- la définition d'une stratégie de ressourcement qui comprend, entre autres:
 - le choix de la stratégie d'assistance à l'IDM entre l'assistance locale et l'assistance à distance;
 - le choix du personnel de soutien, parmi le personnel de l'installation et le personnel du fournisseur;
- le choix des outils de support IDM y compris, entre autres:
 - la décision portant sur les outils de support IDM à utiliser par le projet et l'exploitation/maintenance;
 - la détermination de la disponibilité éventuelle des outils existants et de la nécessité éventuelle de développer de nouveaux outils;
- la détermination des processus de travail y compris, entre autres:
 - la décision portant sur les processus de travail IDM nécessaires au projet et à l'exploitation/maintenance;
 - la détermination des processus de travail des installations existantes qui peuvent être réutilisés avec ou sans modification des processus de travail existants;
 - la définition des rôles et des responsabilités;
 - la détermination des rôles et des responsabilités exigés pour le projet et l'exploitation/maintenance;
 - la détermination des compétences à développer;
 - la définition de la stratégie de maintenance et sa mise en œuvre,
- la détermination, la mise en œuvre et le complément de la structure de gestion du projet et du soutien à long terme.

Les outils IDM doivent être fournis dès le début du cycle de vie du projet (c'est-à-dire, la phase d'élaboration du contenu) et ne pas être reportés jusqu'à la construction ou la mise en service.

Le contenu du projet doit inclure la planification de l'IDM tout au long du cycle de vie d'une installation.

7.3.3 Mise en œuvre de l'IDM dans les installations existantes

L'aptitude et les performances des appareils intelligents actuellement installés et de l'infrastructure associée doivent être déterminées avant de modifier une installation existante qui met en œuvre l'IDM.

NOTE Un audit est un mécanisme couramment utilisé pour déterminer l'aptitude et les performances d'une installation.

La détermination de l'aptitude et des performances doit inclure tous les aspects du programme de maintenance existant, y compris, au minimum, l'équipement, les outils, les compétences et les ressources, les processus de travail et les procédures.

Le plan de mise en œuvre de l'IDM doit intégrer la résolution de toutes les insuffisances constatées lors de l'audit.

Les processus de travail de maintenance doivent être préparés sur la base du programme IDM afin d'atteindre les résultats souhaités dans les installations.

7.3.4 Mise en œuvre des processus de travail IDM dans une installation

L'exigence de mise en œuvre de l'IDM doit être mentionnée dans toutes les demandes de propositions (DP) et tous les contrats qui concernent ou incluent des appareils pour chaque installation.

Un processus de travail IDM doit être défini par son propriétaire, son objectif, ses éléments d'entrée/sortie, son temps de démarrage, les procédures utilisées et leurs interactions pour une installation spécifique.

Les processus de travail IDM doivent être définis et documentés pour chaque phase du cycle de vie de l'installation donnée, conformément au programme IDM de l'entreprise.

Le processus de travail IDM doit être défini sur la base du modèle de processus de travail IDM défini dans le programme IDM en prenant en considération les exigences et les recommandations spécifiées du 8.4 au 8.9 correspondant à la phase du cycle de vie de l'installation.

NOTE Les processus de travail sont différents d'une installation à l'autre. Cette caractéristique entraîne des modifications des modèles de processus de travail génériques utilisés comme base pour le processus de travail mis en œuvre.

Lorsqu'une installation développe ou améliore un processus de travail IDM, ce dernier doit être fondé sur le programme IDM par référence aux modèles de processus de travail IDM définis par le programme IDM.

7.4 Coordination pour une amélioration continue

7.4.1 Généralités

Pour accroître l'efficacité du programme IDM, il convient que les installations partagent les notifications et les solutions correspondantes pour les équipements qui présentent des taux de défaillance anormalement élevés lorsqu'ils sont établis.

Le programme IDM doit inclure un mécanisme de partage des informations entre les installations.

NOTE 1 Les informations et les expériences peuvent être partagées entre l'entreprise et ses installations pour développer et déployer les meilleures pratiques.

NOTE 2 L'un des objectifs du partage d'informations et d'expériences au sein de l'entreprise et de ses installations est de développer et de mettre en œuvre les meilleures pratiques. Le partage d'informations permet d'identifier et d'éviter les risques potentiels.

Des procédures doivent être créées pour contrôler l'efficacité et les performances de l'IDM dans une installation.

NOTE 3 Les IPC constituent un exemple d'outil pour mesurer l'efficacité du programme de contrôle.

NOTE 4 Une première série d'IPC peut concerner l'efficacité du programme et une seconde série d'IPC peut concerner l'efficacité de la mise en œuvre de l'IDM dans l'installation.

Le programme IDM doit établir des mesures quantitatives de ses performances.

NOTE 5 Les mesurages quantitatifs comprennent généralement une méthode convenue pour saisir l'impact potentiel des incidents évités du fait de la modification des pratiques de travail qui découlent de l'utilisation de l'IDM.

Le programme IDM doit identifier et mettre en œuvre les possibilités d'amélioration du programme IDM, des processus de travail, des procédures ou des outils.

Les installations doivent coordonner et maintenir les types et les niveaux des ressources qualifiées pour soutenir l'amélioration continue de l'IDM.

NOTE 6 Les ressources qualifiées comprennent les changements dus à l'évolution du personnel des fournisseurs et du personnel interne, les contrats des fournisseurs, l'introduction de nouveaux outils et de nouvelles technologies, et d'autres perturbations des exigences en matière de compétences.

NOTE 7 Se reporter au 6.3.

7.4.2 Évaluation et audits des activités IDM

La direction de l'entreprise doit effectuer des audits périodiques pour assurer la conformité et la satisfaction des exigences définies par le programme IDM.

NOTE Le respect des objectifs et des calendriers du programme IDM sont des critères d'audit classiques.

Des mécanismes de consignation, tels qu'un tableau de bord, doivent être établis.

Les non-conformités doivent être suivies, signalées et résolues comme cela est stipulé dans le plan qualité du programme IDM.

Les paramètres de mesure du programme (par exemple, les IPC) doivent être évalués en permanence, y compris une revue au niveau de l'entreprise et de l'installation.

7.4.3 Résolution des causes de non-conformités des programmes

Toutes les non-conformités identifiées lors des audits doivent faire l'objet d'une enquête pour déterminer la cause profonde de la non-conformité afin d'éviter qu'elle ne se reproduise.

Les causes systémiques des non-conformités des programmes IDM doivent être résolues au niveau de l'entreprise.

Chaque installation doit fournir une résolution initiale des non-conformités locales et partager avec les autres installations par le biais du processus d'amélioration continue.

NOTE L'opportunité de l'action de résolution peut être déterminée par l'importance de l'appareil:

- impact du dysfonctionnement de l'appareil;
- fréquence et/ou durée de dysfonctionnement de l'appareil; et
- coûts associés au maintien de l'appareil dans un état opérationnel.

7.5 Coordination avec d'autres programmes d'entreprise

7.5.1 Généralités

Les interactions entre les programmes d'entreprise doivent être pleinement définies.

Les objectifs, limites et interfaces de communication entre les programmes d'entreprise concernés doivent être documentés.

7.5.2 Coordination du cycle de vie des activités de programme

La coordination des activités du programme exige une communication entre les différents processus de travail et organisations, qui repose sur l'échange de données et l'utilisation des données qui en résulte pour soutenir les flux de travail associés.

Toutes les organisations doivent coordonner et gérer les transferts de données relatives à l'IDM exigés entre les différents transferts de données tout au long du cycle de vie du projet et de l'installation.

NOTE Les applications et les données associées peuvent passer d'une organisation à une autre au cours du cycle de vie.

7.5.3 Applications

Il convient que les informations relatives à l'IDM soient disponibles pour que les applications puissent les intégrer dans leur exécution.

NOTE 1 Cette disposition exige l'identification des flux de données relatives à l'IDM dès les premières étapes de tout projet qui intègre des appareils intelligents.

EXEMPLE FOUNDATION™ fieldbus¹ propage et utilise le statut des appareils comme partie intégrante de ses algorithmes de commande sur le terrain.

Les exigences des applications doivent être pleinement définies et partagées avec l'IDM pour les exigences relatives aux appareils.

NOTE 2 Les applications définissent les exigences fonctionnelles, de performances et de fiabilité pour les appareils. L'IDM est chargée de déterminer si et comment ces exigences peuvent être satisfaites et de résoudre les différences si elles se produisent.

Les exigences des applications doivent être pleinement définies et partagées avec les systèmes, les réseaux et la sécurité pour la gestion de l'IDM.

NOTE 3 Les applications définissent les exigences fonctionnelles, de performances et de fiabilité pour les réseaux. L'IDM est chargée de déterminer si et comment ces exigences peuvent être satisfaites et de résoudre les différences si elles se produisent.

7.5.4 Informations concernant l'appareil/processus

Il convient que les outils de prise en charge des informations concernant l'appareil et sa configuration soient intégrés aux outils de support des systèmes et des applications, ainsi qu'au modèle d'information global de l'installation.

¹ FOUNDATION™ fieldbus est une appellation commerciale du Groupe FieldComm. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve le détenteur de la marque ou de l'un quelconque de ses produits.

7.5.5 Systèmes, réseaux et sécurité

Des outils et des modèles d'information sont exigés, qui facilitent la coordination entre les fonctionnalités exigées et la gestion des risques, y compris les rôles de tous les participants en matière de cybersécurité.

NOTE L'IDM est responsable de la détermination des informations de sécurité telles que les autorisations d'accès aux appareils.

7.5.6 Phases du cycle de vie

7.5.6.1 Élaboration du domaine d'application

Les outils IDM doivent être suffisamment flexibles pour prendre en charge les mises à jour exigées afin de refléter les changements d'installations et pour s'adapter aux changements de la technologie utilisée pour prendre en charge les informations IDM.

7.5.6.2 EPC

L'entreprise doit définir les informations obligatoires exigées dans le cadre du processus de transfert du projet.

Il convient que l'entreprise indique quel modèle de gestion des données doit être utilisé.

Les organisations EPC doivent gérer et conserver les informations temporaires pendant la période spécifiée dans le contrat.

EXEMPLE Les informations relatives à l'expédition et à la réception associées à l'assemblage des patins ne sont pas exigées par l'installation en exploitation, mais sont nécessaires à la construction par l'EPC.

7.5.6.3 Exploitation et maintenance

Un plan clair de transfert des données entre chaque phase du cycle de vie doit être élaboré.

NOTE Chaque phase du cycle de vie et chaque organisation participante sont susceptibles de présenter des exigences différentes en matière de données et potentiellement des formats de stockage différents.

EXEMPLE Mise hors tension par bloc construit en ligne par des appareils individuels au fur et à mesure de l'opération de maintenance.

7.5.7 Interfaces d'application pour la coordination

L'IDMS doit avoir une interface avec les différentes applications logicielles utilisées par les autres rôles.

8 Phases du cycle de vie de l'installation

8.1 Objectif

Le présent article spécifie les exigences et les recommandations pour atteindre et maintenir l'IDM pour chaque phase du cycle de vie de l'installation.

Le présent article s'applique à toutes les installations qui utilisent des appareils intelligents.

Le présent article spécifie également les exigences et les recommandations pour la gestion, y compris l'élaboration et l'amélioration continue des outils, processus de travail et procédures d'IDM spécifiques à l'installation.

8.2 Généralités

Les processus de travail IDM peuvent être exécutés de manière séquentielle ou simultanée. Il convient de choisir l'exécution séquentielle ou simultanée afin d'optimiser l'allocation des ressources.

NOTE 1 Le modèle de cycle de vie défini dans le présent document présente une série linéaire simplifiée d'activités séquentielles. Le modèle réel d'un cycle de vie de même nature contient un mélange d'activités séquentielles et simultanées.

NOTE 2 De nombreuses activités exigent une itération ou une reprise. L'itération ou la reprise, lorsqu'elles sont associées à des processus de travail simultanés, créent des dépendances entre les activités.

NOTE 3 Le travail simultané peut augmenter la probabilité d'erreurs, d'omissions et de produits incomplets.

Les processus de travail IDM doivent prendre en charge les méthodes de gestion des processus de travail simultanés, indépendants et dépendants.

La reprise ou l'itération doit être terminée et documentée avant la fin d'une activité de travail.

Les processus de travail IDM pour chaque phase du cycle de vie de l'installation doivent être définis par un calendrier approprié afin que les activités exigées puissent être effectuées en temps voulu et correctement.

Les processus de travail IDM doivent être maintenus et améliorés en permanence, conformément à la MOC de l'installation.

8.3 Gestion des phases du cycle de vie de l'installation

8.3.1 Généralités

Les buts, objectifs, activités et ressources, ainsi que l'état d'avancement de toute entreprise dans chaque phase du cycle de vie de l'installation doivent être organisés et contrôlés par un système de gestion.

NOTE 1 Les phases du cycle de vie fournissent un moyen pratique de communiquer l'état et les actions du cycle de vie aux groupes concernés dans le but de gérer les activités et les ressources. Les limites du cycle de vie se chevauchent parfois ou varient en fonction de la culture organisationnelle et des caractéristiques individuelles du cycle de vie.

NOTE 2 La gestion du cycle de vie permet de déterminer les exigences en matière de ressources et de responsabilités pour les activités qui ne relèvent pas des limites de l'exploitation et de la maintenance normales d'une installation, et pour les modifications d'ingénierie ou de conception dans le cadre des activités d'exploitation et de maintenance.

Les rôles et les responsabilités de tous les participants doivent être attribués et coordonnés tout au long du cycle de vie de l'installation par un système de gestion.

La méthodologie et la responsabilité de la gestion des activités du cycle de vie doivent être documentées et communiquées à tous les participants.

Le programme IDM doit être mis en œuvre pour prendre en charge toutes les phases du cycle de vie, y compris l'obsolescence.

Un système de gestion des données est exigé pour permettre une documentation adéquate de toutes les phases du cycle de vie.

8.3.2 Points d'entrée du cycle de vie

Les processus de gestion des installations doivent s'adapter aux changements ou aux perturbations d'origine interne ou externe qui créent un besoin de travail en dehors de la phase active actuelle du cycle de vie des installations.

NOTE 1 Les changements peuvent provenir de modifications simples ou complexes des installations, de l'évolution de la technologie des appareils ou de la simple migration des révisions des appareils. Lorsque les changements sont simples, répétitifs et peuvent être partiellement automatisés, ils peuvent être définis à l'avance comme une pratique ou une procédure de travail et mis en œuvre avec un impact minimal.

NOTE 2 Certains changements, comme le remplacement en nature d'un appareil, peuvent être réalisés au cours d'une seule phase du cycle de vie.

Dans chaque cas pour lequel des changements sont exigés, un processus formel doit être utilisé pour déterminer quelles activités du cycle de vie sont nécessaires pour soutenir le changement et quel est le point de départ du cycle de vie approprié pour gérer le changement associé.

8.3.3 Modifications des installations

Une revue technique et de direction appropriée doit être effectuée pour apprécier le risque associé aux évolutions du domaine d'application avant de mettre en œuvre tout changement.

Tout changement concernant l'ingénierie de l'installation doit être documenté, et une formation appropriée portant sur les changements observés doit être suivie avant leur mise en œuvre.

Un processus MOC est exigé, mais il peut être et est souvent unique à chaque entreprise ou installation.

NOTE 1 Certaines modifications d'installation sont de simples remplacements fonctionnels pour la réparation de composants défectueux. Certains de ces remplacements peuvent avoir une gestion du cycle de vie très simple, définie par les politiques de l'installation.

NOTE 2 Certaines de ces modifications simples peuvent être reproduites pour de nombreuses applications d'équipements couramment utilisés, y compris l'utilisation commune de l'ingénierie et de la documentation pour les modifications reproduites. Les programmes IDM peuvent faciliter la reproduction et le partage.

NOTE 3 Des informations supplémentaires concernant les exigences fondamentales de la MOC sont fournies au 4.5.

8.4 Élaboration du domaine d'application

8.4.1 Généralités

Lors du transfert de la phase d'élaboration du domaine d'application à la phase de "conception et d'ingénierie", les résultats minimaux suivants doivent être fournis au minimum:

- les catégories des appareils intelligents;
- l'architecture/schéma fonctionnel du système de gestion des appareils intelligents;
- un audit des aptitudes des appareils intelligents actuellement installés et de l'infrastructure associée;
- une liste des écarts par rapport au programme IDM;
- les spécifications propres à l'IDM.

NOTE 1 Une liste type des spécifications concernées par l'IDM et qui sont exigées est donnée ci-dessous:

- instruments numériques et spécification des contrôleurs de vannes – Cette spécification peut être couverte dans une section spécifique du projet Spécifications des vannes d'instrumentation et de commande;
- spécification de l'instrumentation sans fil;
- spécification des appareils électroniques intelligents;
- spécification d'intégration d'un appareil intelligent et d'un système de gestion d'un appareil;
- spécification de cybersécurité des systèmes OT.

NOTE 2 Le document de spécification de la cybersécurité des systèmes OT peut être développé par d'autres dans le cadre de normes de cybersécurité plus larges. Toutefois, l'équipe du projet IDM vérifie également que le document intègre les exigences en matière de cybersécurité de l'IDM.

Les processus de travail IDM suivants doivent être définis pour les activités IDM exécutées dans la phase d'élaboration du domaine d'application:

- planification et conception pour la mise en œuvre de l'IDM;
- résultat d'analyse du classement par criticité;
- définition d'une stratégie de soutien à long terme (stratégie de soutien technique);
- choix de solutions alternatives de conception;
- préparation des outils (processus de travail de base) et leurs procédures;
- choix des fournisseurs;
- développement d'une stratégie de cybersécurité;
- planification de transfert.

NOTE 3 Les dispositions relatives à ces processus de travail IDM sont spécifiées dans les paragraphes suivants.

NOTE 4 Des processus de travail IDM supplémentaires peuvent être définis pour cette phase du cycle de vie des installations.

Les processus de travail IDM pour la définition et la documentation des fonctionnalités des IACS et des appareils intelligents doivent au minimum être définis pour les conditions de fonctionnement suivantes:

- fonctionnement normal;
- fonctionnement anormal; et
- traitement des pannes ou des défaillances.

NOTE 5 Les processus et procédures de travail pour la définition des exigences fonctionnelles ne relèvent pas du domaine d'application du présent document, mais les résultats de ces processus sont considérés comme des données exigées pour l'IDM.

Des exigences doivent être définies et documentées pour les performances des IACS et des appareils intelligents.

NOTE 6 Les mesures de performances comprennent, entre autres, la vitesse et la répétabilité.

Des exigences et des plans spécifiques doivent être identifiés et documentés pour la cybersécurité, y compris des processus et des procédures de travail compensatoires pour les appareils intelligents qui ne prennent pas en charge la cybersécurité.

NOTE 7 Les appareils intelligents peuvent introduire des failles de sécurité dans l'IACS.

NOTE 8 Les exigences en matière de cybersécurité sont définies dans la série IEC 62443.

Les appareils intelligents doivent indiquer quelles fonctions de l'appareil sont exigées pour l'application.

NOTE 9 Un seul appareil intelligent peut avoir de nombreuses options de configuration de notification. Le fait que la justification des instruments pour les appareils intelligents ne comporte pas d'informations détaillées suffisantes peut contribuer à l'inondation d'alarmes et d'alertes au cours des dernières phases du projet.

NOTE 10 La classification de la notification dépend du rôle de l'appareil, ainsi que de la conséquence des informations de diagnostic sur l'état de fonctionnement de l'appareil.

NOTE 11 Pour éviter les notifications intempestives, il est nécessaire de désactiver les fonctions non indiquées dans l'appareil intelligent.

Les outils IDM doivent être fournis dès le début du cycle de vie du projet (c'est-à-dire, la phase d'élaboration du domaine d'application) et ne pas être reportés jusqu'à la construction ou la mise en service.

Les exigences en matière d'IDM doivent être incluses dans l'élaboration du domaine d'application d'une installation.

NOTE 12 Les exigences en matière d'IDM constituent une composante de l'ensemble du domaine d'application d'une installation.

8.4.2 Objectif

L'objectif des exigences du 8.4.1 est de catégoriser les applications de l'appareil intelligent, y compris les notifications générées par ce dernier, de manière à soutenir durablement les activités de l'IDM en matière d'ingénierie, d'exploitation et de planification de la maintenance.

8.4.3 Gestion des risques

8.4.3.1 Généralités

L'appréciation du risque doit être complète et documentée avant les activités de conception de l'IDM.

NOTE 1 L'appréciation du risque ne relève pas du domaine d'application du présent document et constitue une condition préalable importante de l'IDM qui est réalisée pendant la phase d'élaboration du domaine d'application.

NOTE 2 L'appréciation du risque peut utiliser différentes techniques, y compris, entre autres: Le classement par criticité, LOPA, l'arbre de panne et la modélisation de Markov.

NOTE 3 Le présent document ne spécifie pas d'exigences ou de recommandations concernant ces techniques d'évaluation. D'autres normes telles que la norme ISA84 fournissent des recommandations.

8.4.3.2 Analyse de l'appréciation du risque

L'analyse de l'appréciation du risque permet de déterminer la criticité des appareils. Elle doit être achevée avant le début de la conception détaillée.

NOTE De nombreux choix de conception dépendent de la criticité des appareils. En général, le programme IDM définit des règles et des méthodes pour la conception des appareils intelligents qui couvrent des circonstances spécifiques dans lesquelles la cohérence est importante (par exemple, les protocoles de communication) en fonction du classement par criticité.

L'approche utilisée dans la spécification, la conception et la mise en œuvre d'un appareil intelligent doit être conforme aux attentes définies sur la base du classement par criticité et de la classification de notification de l'appareil intelligent pour cette installation.

Les informations spécifiques à l'installation concernant les solutions alternatives de conception doivent être conservées de manière à pouvoir survivre aux changements de personnel.

8.4.4 Considérations relatives au type de projet

Les activités d'élaboration de contenu du projet et d'ingénierie doivent être adaptées au type de projet.

NOTE Des activités supplémentaires d'élaboration du contenu et d'ingénierie sont nécessaires pour les modifications des installations qui ne sont pas pertinentes pour la création de nouvelles installations.

Les projets qui prévoient la modification d'installations existantes doivent assurer que tout équipement qui sera réutilisé est adapté aux nouvelles conditions de service.

Les principes de conception et les décisions relatives à l'élaboration du contenu doivent être conservés de manière à soutenir la gestion des changements à long terme.

Si tel n'est pas le cas, l'infrastructure exigée doit être intégrée dans le contenu du projet initial.

8.4.5 Planification et conception de la mise en œuvre de l'IDM

Un plan de mise en œuvre de l'IDM doit être défini et documenté pour atteindre les exigences en matière d'IDM définies au 9.4.

Il convient de définir et d'exécuter un processus de travail en matière de planification et de conception pour la mise en œuvre de l'IDM au début de la phase d'élaboration du domaine d'application.

Le processus de travail de planification et de conception de la mise en œuvre de l'IDM doit être cohérent avec le programme IDM de l'entreprise.

Le plan documenté de mise en œuvre de l'IDM doit comporter les éléments suivants:

- portée détaillée de la mise en œuvre de l'IDM;
- processus de travail IDM à définir;
- ressources estimées exigées pour chaque phase du cycle de vie de l'installation;
- liste des normes, spécifications, règlements et codes applicables à la mise en œuvre de l'IDM;
- résultats du classement par criticité.

Le plan documenté de mise en œuvre de l'IDM peut également comporter les éléments suivants:

- formule des IPC et valeurs cibles.

Les éléments d'entrée du processus de travail de planification et de conception de la mise en œuvre de l'IDM doivent comporter:

- les objectifs de la mise en œuvre de l'IDM;
- les exigences des programmes IDM de l'entreprise;
- le concept de fonctionnement de l'installation;
- le concept de maintenance de l'installation;
- le plan d'exécution du projet de l'installation;
- la limitation des ressources;
- le résultat de l'appréciation du risque.

Les éléments d'entrée supplémentaires peuvent inclure:

- les performances attendues (IPC) de l'IDM.

NOTE Un plan qui vise à satisfaire aux exigences en matière d'IDM fait généralement partie d'un plan de projet.

8.4.6 Définition de plans de soutien à long terme de l'installation

Si le processus de travail IDM du plan de soutien à long terme de l'installation n'est pas défini dans le programme IDM, il doit l'être dans le processus de travail de planification et de conception de la mise en œuvre de l'IDM.

Un plan de soutien à long terme de l'installation doit être défini afin de maintenir la conformité aux exigences en matière d'IDM définies au 8.3 pendant toute la durée de vie de l'installation.

Les plans de soutien à long terme de l'installation doivent inclure, au minimum, les plans de ressources en personnel local ou distant, les rôles et les responsabilités, le soutien extérieur (tiers) et le soutien de l'entreprise, y compris le soutien au niveau du programme.

NOTE 1 Les processus et procédures de travail IDM constituent une partie essentielle du plan de soutien à long terme de l'installation. Certains de ces processus et procédures de travail peuvent être fournis par un programme IDM.

Le résultat du processus de travail IDM qui porte sur la définition du plan de soutien à long terme de l'installation doit être documenté pour le soutien à long terme des appareils intelligents.

NOTE 2 Le plan documenté de soutien à long terme de l'installation propre aux appareils intelligents comprend:

- un plan de dotation en personnel concernant l'assistance locale et/ou à distance;
- une structure coopérative d'assistance locale et à distance avec des rôles et des responsabilités clairs pour chacun;
- une charte de l'équipe;
- des parcours de formation et d'apprentissage.

Les éléments d'entrée du processus de travail IDM qui vise à définir le plan de soutien à long terme de l'installation doivent comprendre les éléments suivants:

- programme de maintenance de l'installation;
- programme IDM;
- plan de mise en œuvre de l'IDM;
- plan du projet de mise en œuvre de l'installation;
- stratégie documentée de classement par criticité des appareils intelligents.

8.4.7 Plan de transfert à l'exploitation et à la maintenance

Un plan de transfert doit être défini et documenté.

Le plan de transfert doit assurer la continuité de la conformité aux exigences.

NOTE Le transfert représente une discontinuité naturelle du personnel, des outils, des processus et des procédures de travail. Les plans de transfert peuvent inclure la formation du personnel de soutien à long terme et le transfert vers différents systèmes de gestion de l'information.

Le plan de transfert doit:

- a) identifier les dossiers permanents à transférer du projet à l'installation;
- b) identifier le format des dossiers permanents à transférer;
- c) fournir un état complet des tâches et des produits livrables;
- d) fournir une liste des activités ou des points d'action laissés en suspens;
- e) dresser une liste des activités immédiates et des enjeux potentiels en fonction de l'état des produits livrables et des actions en cours.

Le plan de transfert documenté relatif aux appareils intelligents doit inclure les éléments suivants:

- données de configuration;
- modèles;
- plan général de transfert, y compris le personnel de formation et de soutien;
- formulaire de gestion de la documentation et de l'information;
- gestion des changements/revue de prédémarrage.

Les éléments d'entrée du processus de travail IDM du plan de transfert doivent comprendre les éléments suivants:

- programme IDM;
- plan de mise en œuvre de l'IDM;
- plan du projet de mise en œuvre de l'installation;
- stratégie documentée de classement par criticité des appareils intelligents;
- stratégie documentée pour le soutien à long terme des appareils intelligents.

Il convient que le temps de démarrage du plan de transfert constitue le moment auquel le plan de mise en œuvre de l'IDM est disponible.

8.4.8 Définition d'une stratégie de cybersécurité pour les appareils intelligents

8.4.8.1 Généralités

Le résultat du processus de travail IDM d'élaboration d'une stratégie de cybersécurité doit être une stratégie documentée pour la cybersécurité liée aux appareils intelligents.

NOTE 1 La série IEC 62443 fournit des exigences en matière de cybersécurité pour les appareils, les systèmes et les procédures ou processus de travail employés dans l'automatisation industrielle.

NOTE 2 Ces exigences peuvent être simplifiées à l'aide d'outils modernes, ou elles peuvent être satisfaites par des procédures manuelles. Les procédures manuelles peuvent s'avérer difficiles dans certaines conditions.

NOTE 3 Il n'existe pas d'exemption pour les appareils qui ne sont pas conçus pour fournir des outils de support à la cybersécurité.

NOTE 4 La série IEC 62443 exige l'application d'un programme de cybersécurité afin d'assurer l'efficacité des mesures de même nature. L'IDM dépend de l'efficacité du programme de cybersécurité.

L'IDM doit fournir un soutien pour les fonctions de cybersécurité, y compris, au minimum, l'authentification, l'autorisation, la journalisation et la sauvegarde/restauration.

8.4.8.2 Authentification

Les mesures d'authentification doivent empêcher l'accès anonyme ou frauduleux aux logiciels, au matériel ou aux personnes.

NOTE 1 Les composants modernes sont accompagnés de certificats et d'un stockage inviolable pour assurer l'authenticité et une chaîne de confiance.

NOTE 2 Les systèmes modernes fournissent une connexion fondée sur les rôles avec une authentification à un ou plusieurs facteurs.

NOTE 3 Les outils portables ne fournissent pas d'outils pour répondre à cette exigence et des procédures manuelles sont exigées pour combler ce vide si des outils portables sont utilisés.

8.4.8.3 Autorisation

L'autorisation doit être utilisée pour fournir un moyen de gestion des changements (MOC).

NOTE 1 L'autorisation n'a pas de sens sans l'authentification.

NOTE 2 De nombreux outils portables ne satisfont pas à cette exigence sans procédures manuelles.

NOTE 3 Les procédures manuelles sont généralement moins efficaces et plus lourdes que les procédures qui utilisent le type et les quantités corrects d'outils.

L'autorisation doit fournir un contrôle d'accès pour la visualisation et la modification du matériel, du logiciel, de la configuration ou des paramètres de fonctionnement.

Un contrôle d'accès doit être prévu pour les appareils, les systèmes et les utilisateurs.

Le contrôle de l'accès doit être assuré par des outils et des procédures appropriés.

NOTE 4 Les certificats et les systèmes de gestion des certificats constituent un moyen d'assurer la sécurité et l'authenticité des données échangées.

L'autorisation doit être fondée sur les rôles.

8.4.8.4 Journalisation

La journalisation doit permettre de conserver les changements sous forme de dossier.

NOTE 1 La plupart des appareils intègrent un compteur de changement pour faciliter l'intégrité de cette fonction.

NOTE 2 De nombreux systèmes hôtes avec des appareils connectés en permanence peuvent simplifier ou automatiser cette fonction.

NOTE 3 Cette fonction est plus complexe et moins fiable lorsqu'elle dépend d'outils de configuration portatifs.

8.4.8.5 Sauvegarde et restauration

Les fonctions de sauvegarde et de restauration doivent être utilisées pour fournir une sauvegarde de la configuration actuelle de l'appareil et la possibilité de restaurer cette configuration si nécessaire.

NOTE 1 De nombreux systèmes hôtes avec des appareils connectés en permanence peuvent simplifier ou automatiser cette fonction.

NOTE 2 Cette fonction est plus complexe et moins fiable lorsqu'elle dépend d'outils de configuration portatifs.

La stratégie relative aux éléments d'entrée de cybersécurité doit comprendre:

- des politiques et des lignes directrices de cybersécurité de l'installation pour le domaine OT;
- un programme IDM;
- un plan de mise en œuvre de l'IDM;
- un plan du projet de mise en œuvre de l'installation;
- une stratégie documentée de classement par criticité des appareils intelligents;
- une stratégie documentée pour le soutien à long terme des appareils intelligents.

8.4.9 Choix de solutions alternatives de conception

Une stratégie de choix de solutions alternatives de conception doit être documentée, y compris:

- le regroupement des fonctions;
- la liste des technologies agréées;
- des solutions alternatives de conception pour chaque groupe de fonctions;
- des critères d'évaluation pour le choix des solutions alternatives;
- la liste de pratiques de conception ou de conceptions d'équipement nouvelles ou non éprouvées;
- la liste des nouvelles technologies candidates et taux d'adoption par le secteur;
- les matrices de comparaison des technologies;
- une méthode systématique de conservation des informations relatives à l'évaluation des technologies;
- un plan de formation et de soutien externe pour le personnel impliqué dans la conception et l'ingénierie.

Les éléments d'entrée du processus de travail IDM pour le choix de solutions alternatives de conception doivent comprendre les éléments suivants:

- un programme IDM;
- un plan de mise en œuvre de l'IDM;
- plan du projet de mise en œuvre de l'installation;
- une stratégie documentée de classement par criticité des appareils intelligents;
- une stratégie documentée pour le soutien à long terme des appareils intelligents.

Le choix de la technologie doit prendre en considération la spécification des exigences fonctionnelles de l'application et le processus de travail IDM défini, y compris les exigences en matière d'opérabilité et de maintenabilité durables.

Le choix entre les solutions alternatives de conception doit inclure une évaluation des risques, ainsi que des avantages du choix de la conception ou de la technologie.

NOTE 1 Le choix de "cloner" une conception existante peut réduire le risque. En variante, la conception clonée peut introduire une obsolescence au début du cycle de vie de l'installation.

Les plans d'introduction de nouvelles technologies doivent inclure l'identification des besoins en nouveaux outils, compétences et formations, ainsi que des plans pour répondre à ces besoins d'amélioration des infrastructures locales existantes (vertes ou brunes) et des plans destinés à combler les besoins identifiés.

NOTE 2 Le plan peut inclure le soutien du programme IDM pour l'introduction de nouveaux outils et l'élaboration de nouveaux processus de travail. Les outils et les processus de travail développés en dehors de l'installation sont souvent utiles.

NOTE 3 L'infrastructure locale comprend généralement la fourniture d'équipements et de services en dehors de l'installation qui peuvent être utilisés pour le soutien de cette dernière.

Le soutien à long terme (c'est-à-dire les normes comme base à assurer), le modèle de maturité et la stabilité doivent être évalués dans le processus de sélection.

8.4.10 Préparation des outils et de leurs procédures

Le résultat du processus de travail IDM de préparation des outils (processus de travail de base) et de leurs procédures doit être le suivant:

- outils pour l'IDM;
- procédures d'emploi des outils;
- processus de travail IDM pour la maintenance des outils;
- plans de formation.

Des outils pour chaque phase du cycle de vie doivent être fournis.

Les outils doivent pouvoir être utilisés pour les installations existantes.

Il convient que les outils comprennent:

- un outil de gestion des données de configuration des appareils intelligents;
- un outil de configuration des appareils intelligents;
- un outil de remplacement des appareils intelligents.

Les outils existants peuvent être réutilisés.

Une procédure de chaque outil pour chaque phase du cycle de vie doit être fournie.

Il convient que le plan de formation des outils comprenne:

- des documents de formation;
- les jalons du cycle de vie de l'installation;
- les procédures de gestion des compétences du personnel.

Les éléments d'entrée pour la "préparation des outils (processus de travail de base) et de leurs procédures" doivent être les suivants:

- un programme IDM;
- un plan de mise en œuvre de l'IDM;
- un plan du projet de mise en œuvre de l'installation;
- une stratégie documentée de classement par criticité des appareils intelligents;
- une stratégie documentée pour le soutien à long terme des appareils intelligents;
- une stratégie documentée de choix des solutions alternatives de conception.

La prise en charge par le système de l'exportation, de l'importation et de la compilation globale (hors ligne - sans appareil connecté) des fonctions IDM doit être prise en considération dans la conception et l'ingénierie des IACS.

NOTE 1 La compilation globale est généralement utilisée dans les projets de mise en œuvre de grandes installations.

NOTE 2 L'utilisation de modèles d'appareils intelligents ou d'informations de configuration peut favoriser la cohérence des paramètres détaillés entre des familles d'appareils similaires.

La prise en charge par le système de la configuration en ligne (appareil connecté) doit être prise en considération dans la conception et l'ingénierie des systèmes d'appareils intelligents.

Les outils d'ingénierie et de maintenance ainsi que les procédures associées doivent être identifiés et mis en œuvre avant l'achèvement du projet.

NOTE 3 L'identification des outils d'ingénierie et de maintenance et des procédures associées pendant l'élaboration du contenu du projet rend le processus de conception plus efficace et réduit les erreurs d'omission.

Des exigences doivent être définies et documentées pour un processus et des procédures de travail applicables au remplacement des appareils.

NOTE 4 Le remplacement peut être exigé une ou plusieurs fois au cours de toute phase du cycle de vie d'une installation.

NOTE 5 Les appareils de remplacement contiennent souvent des mises à jour ou des révisions logicielles. Un programme peut fournir une assistance pour les mises à jour logicielles ou la migration des configurations.

NOTE 6 Les changements de technologie ou de fournisseur d'appareils ne relèvent pas du domaine d'application des plans normaux de remplacement des appareils. Un programme peut fournir une assistance pour les changements de technologie ou de fournisseur.

8.4.11 Choix des fournisseurs

Le résultat du processus de travail IDM pour le choix des fournisseurs doit être une liste des fournisseurs agréés (AVL) pour chaque catégorie d'appareil intelligent, qui peut également inclure les numéros de modèle recommandés.

Ce processus de travail doit prendre en considération les exigences en matière d'acquisition et de chaîne logistique.

Chaque élément de la liste des AVL doit comprendre au minimum les éléments suivants:

- type d'application (par exemple, instrumentation, circuits électriques, analyse des processus);
- nom et coordonnées du fournisseur;
- catégorie d'appareil intelligent (analytique, débit, pression, température, vanne, etc.);
- groupes fonctionnels (classes principales d'équipements, de technologies et/ou de services).

Des exigences doivent être définies et documentées pour les choix des fournisseurs.

NOTE 1 Les éléments identifiés comme des produits de base peuvent parfois être sélectionnés après l'élaboration du domaine d'application.

NOTE 2 Les éléments qui exigent un effort d'ingénierie et l'intégration des IACS bénéficient d'une sélection précoce et d'une planification du soutien du cycle de vie complet.

NOTE 3 Les choix des fournisseurs peuvent être proposés par un programme IDM.

8.4.12 Planification de la gestion de l'information

Les informations issues de l'élaboration du domaine d'application et des phases ultérieures du cycle de vie doivent être classées comme dossiers permanents ou dossiers temporaires.

Les informations identifiées comme un dossier permanent doivent être fournies sous une forme qui peut être conservée tout au long du cycle de vie de l'installation.

NOTE 1 Ce cycle de vie peut s'étendre sur plus de 50 ans et représente un enjeu pour les supports électroniques. Il représente également un enjeu pour le maintien des compétences nécessaires à l'utilisation des informations.

NOTE 2 La gestion de l'information utilise souvent différents outils, processus de travail et compétences au cours des différentes phases du cycle de vie d'une installation. La continuité, l'intégrité et la longévité sont les clés du succès.

NOTE 3 Il est possible que certains des outils et des compétences nécessaires à la conservation des informations ne soient pas présents dans une installation.

NOTE 4 Les appareils intelligents exigent la gestion d'un plus grand nombre de données que les anciens types d'appareils.

Les informations à gérer doivent comprendre, au minimum, les données, schémas, calculs, modèles et autres informations et compétences nécessaires pour gérer et valider les modifications de conception tout au long du cycle de vie de l'installation.

Une méthode systématique de conservation des informations relatives aux spécifications, à la conception (y compris les solutions alternatives de conception) et à la mise en œuvre de l'appareil intelligent tout au long du cycle de vie de l'application doit être établie. Il convient que la méthode utilisée pour conserver cette information reste efficace malgré les changements de personnel.

NOTE 5 L'établissement d'une méthode cohérente de documentation des informations détaillées de la spécification, de la conception et de la mise en œuvre des appareils intelligents favorise la réussite du projet IDM et l'intégrité à long terme des données de l'installation.

NOTE 6 Se reporter à l'Article 10 pour une description détaillée de la gestion de l'information.

8.5 Conception et ingénierie

8.5.1 Objectif

Le présent paragraphe (8.5) a pour objectif de vérifier que des informations de conception détaillées suffisantes sont élaborées pour soutenir l'acquisition, la construction, l'installation, la mise en service, l'exploitation et la maintenance des appareils intelligents d'une manière conforme aux exigences définies du programme, du système de gestion et des spécifications fonctionnelles.

8.5.2 Généralités

Avant d'entrer dans cette phase, les éléments d'entrée suivants doivent être fournis:

- a) contenu et objectifs du projet;
- b) références aux normes du projet/de l'installation, lignes directrices et processus de travail;
- c) documents conceptuels du projet/de l'installation (tels que les schémas fonctionnels, les stratégies de protection et les concepts de maintenance);
- d) liste préliminaire des équipements du projet/de l'installation (index des instruments, tableau de commande de moteur, système d'analyse, etc.).

Lors du transfert de cette phase à la construction et à la mise en service, les éléments de sortie suivants doivent être fournis:

- spécification de la conception fonctionnelle du système de gestion des appareils et plan d'essai IACS;
- liste des appareils (comprend le fournisseur de l'appareil, le modèle, les quantités, etc.);
- base de données de configuration de l'appareil (qui comprend les fiches techniques);
- schémas de câblage des appareils et plans de câbles;
- plans de réseaux, schémas fonctionnels de réseaux (réseaux de communication, principaux composants généraux, etc.);
- classement final par criticité de l'appareil (cybersécurité et maintenance) si les classements initiaux ont été modifiés au cours de la conception et de l'ingénierie;
- stratégie en matière de pièces de rechange alignée sur la stratégie de maintenance;
- plan de formation et de qualifications pour l'équipe ou les équipes de l'installation;
- diagrammes de flux de travail associés au contrôle de boucle de l'appareil et à la mise en service.

Les processus de travail IDM suivants doivent être définis comme les activités IDM exécutées dans cette phase du cycle de vie de l'installation:

- choix du fournisseur final;
- choix de l'appareil individuel;
- acquisition d'appareils intelligents;
- coordination avec les fonctions IACS connexes;
- spécification des processus de travail pour la phase d'exploitation et de maintenance;
- préparation des modèles de configuration des appareils;
- préparation des données de configuration (à l'aide de modèles dans toute la mesure du possible);
- plans de vérification et d'essai de la configuration, y compris FAT, SAT.

NOTE 1 Les dispositions relatives à ces processus de travail IDM sont spécifiées dans les paragraphes suivants.

D'autres processus de travail IDM associés à cette phase du cycle de vie des installations peuvent être définis en plus de ceux énumérés ci-dessus.

EXEMPLE Conception présumée du fournisseur et formation des compétences prévues.

La gestion détaillée de la configuration avec vérification et non-remplacement en nature doit avoir un identificateur unique d'appareil intelligent.

L'entreprise doit établir un système qui permet d'obtenir des identificateurs uniques d'appareils intelligents à l'échelle de l'entreprise.

NOTE 2 Les noms d'étiquettes constituent une forme d'identificateurs uniques d'appareils.

La conception de la configuration détaillée d'un appareil intelligent doit fournir tous les paramètres configurables de l'appareil intelligent et la configuration IACS associée, nécessaires pour réaliser la fonctionnalité spécifiée.

NOTE 3 Les modèles et les outils agréés pour les appareils intelligents, fondés sur les classements par criticité définis, peuvent soutenir la conception détaillée de la majorité des paramètres des appareils intelligents.

La spécification des exigences relatives à l'appareil intelligent doit comporter des informations suffisantes pour assurer que la conception et la mise en œuvre détaillées de l'appareil intelligent correspondent à l'intention et à l'approche documentées lors de l'identification, de la justification et du classement par criticité dudit appareil.

8.5.3 Choix d'un appareil

8.5.3.1 Généralités

Il convient de définir le processus de travail IDM pour le choix d'un appareil avant le début de la phase de conception et d'ingénierie.

Les critères de choix d'un appareil intelligent doivent être définis dans le processus de travail IDM pour le choix d'un appareil.

Les critères de choix d'un appareil intelligent doivent inclure les exigences spécifiées en matière de fonctionnalité de l'appareil intelligent et de l'IDM (telles que les notifications d'état et de diagnostic) nécessaires pour atteindre et maintenir les performances exigées de l'appareil intelligent et de l'IDM, en plus des exigences relatives aux fonctions primaires de l'appareil (par exemple, les fonctions primaires définies par les ingénieurs de conception des instruments). Les exigences en matière d'IDM doivent être mentionnées dans la première et l'ensemble des DP, ainsi que dans les contrats associés qui concernent ou incluent des appareils pour chaque installation.

Les exigences concernant l'opérabilité, la maintenabilité, les diagnostics, les examens et la testabilité doivent être prises en compte lors de la conception de l'application de l'appareil intelligent afin de réduire la probabilité de défaillances dangereuses.

Le résultat du processus de travail IDM pour le choix d'un appareil doit prendre la forme d'une liste des appareils intelligents et des fonctionnalités IDM exigées pour chaque type d'appareil en fonction de son classement par criticité.

NOTE 1 Le classement par criticité est décrit à l'Annexe D de l'IEC TR 63082-1:2020.

NOTE 2 L'activité de choix d'un appareil ne définit pas la criticité de l'appareil en soi, mais spécifie la fonctionnalité de l'appareil intelligent (diagnostic exigé, etc.) pour les appareils d'une criticité donnée.

8.5.3.2 Liste des exigences relatives au choix d'un appareil

La liste des exigences relatives au choix d'un appareil doit inclure les éléments suivants:

- description de la ou des fonctionnalités spécifiques de l'appareil intelligent;
 - exigences en matière d'opérabilité, de maintenabilité, de diagnostic, d'examens et de testabilité,
 - critères de choix et principes de conception des appareils intelligents;
- description de la ou des fonctionnalités spécifiques de l'IDM;
- technologies des appareils (pression, température, etc.);
- classement par criticité;
- protocoles de communication sur le terrain;
- vérification de la compatibilité avec le système hôte;
- identification/présélection effectives du fabricant/modèle des appareils;
 - fabricant,
 - nom de modèle de l'appareil choisi,
 - spécification de l'appareil (par exemple, numéro de modèle, numéro de pièce pour une description complète de l'appareil),
 - fournisseur,
 - outils utilisés pour l'appareil,
 - caractéristiques de base ou facultatives (c'est-à-dire, les diagnostics qui ne figurent pas dans le numéro du modèle de base),
 - traitement des défaillances (par exemple, NAMUR NE 043),
 - messagerie de diagnostics (par exemple, NAMUR NE 107),
 - documentation exigée (par exemple, examen, outils et leurs procédures d'emploi).

NOTE 1 Détermination des nouveaux types d'outils, dont il est peu probable que l'installation en dispose déjà, nécessaires à la prise en charge l'appareil.

NOTE 2 Les fonctionnalités disponibles des appareils intelligents et de l'IDM sont prédéterminées lorsqu'il n'existe qu'un seul modèle d'appareil agréé pour le classement par service/criticité.

Lors de l'établissement des listes des appareils choisis, il convient de prendre en considération les changements au niveau du personnel, des outils, des processus et des procédures de travail.

Les appareils intelligents et les outils destinés à ces appareils doivent être intégrés et configurés de manière correcte.

Il convient d'identifier et de convenir de la capacité de l'installation à prendre en charge chaque type d'appareil intelligent le plus tôt possible dans le processus de conception.

NOTE 3 Le choix d'appareils toujours en cours d'élaboration ou dont la technologie est nouvelle pour l'installation expose cette dernière à un risque supplémentaire qui exige des efforts particuliers en matière de gestion et d'essais.

Les éléments d'entrée du processus de travail IDM pour le "choix d'un appareil" doivent comprendre les éléments suivants:

- un programme IDM;
- un plan de mise en œuvre de l'IDM;
- un plan de mise en œuvre du projet de l'installation;
- une stratégie documentée de classement par criticité des appareils intelligents;
- une stratégie documentée pour le soutien à long terme des appareils intelligents;
- la spécification des exigences fonctionnelles pour chaque type d'appareil intelligent.

Il convient que les critères de choix et les principes de conception comprennent les éléments suivants:

- le rôle du système hôte des appareils intelligents dans l'identification des approches d'un fonctionnement dangereux ou anormal, dans l'avertissement des dysfonctionnements et dans l'incitation à prendre des mesures;
- les méthodes à appliquer pour l'identification des appareils intelligents;
- les états de l'appareil intelligent (par exemple, normal, acquitté, en suspens, etc.) que l'installation utilisera.

8.5.4 Acquisition de l'appareil intelligent

8.5.4.1 Généralités

Il convient de définir le processus de travail IDM pour l'acquisition d'un appareil dès le début de la phase de conception et d'ingénierie.

La conception détaillée de l'installation de l'appareil intelligent doit être conforme à la spécification des exigences fonctionnelles dudit appareil, tout en prenant également en considération les exigences du 8.5.4. Le type d'appareil peut être obtenu auprès de plusieurs fournisseurs, et la restriction portant sur le choix des fournisseurs fait partie du processus d'acquisition.

L'entreprise doit identifier les critères de choix et les principes de conception des appareils intelligents, conformément à la définition d'un appareil intelligent et aux exigences du programme IDM.

Le résultat du processus de travail IDM pour l'acquisition d'un appareil intelligent doit constituer les étapes d'acquisition des appareils intelligents et des informations associées pour chaque appareil exigé. Les informations associées doivent comprendre les éléments suivants:

- fabricant de l'appareil acquis;
- fournisseur de l'appareil acquis;
- numéro de modèle de l'appareil acquis;
- identificateur unique (par exemple, numéro d'étiquette, numéro de série) de l'appareil individuel acquis;
- informations concernant la configuration de l'appareil;
- essai de vérification de l'appareil dans le conteneur d'expédition;
- informations concernant la certification et l'homologation de l'appareil;
- fichiers de support de l'appareil (par exemple, EDD, DTM);
- manuels de service et de dépannage des appareils.

L'acquisition doit s'effectuer sur la base des exigences définies par le projet et confirmées par le fabricant.

La configuration des appareils avant leur arrivée sur site peut être prise en considération. Dans ce cas, il convient que la spécification d'acquisition de l'appareil contienne les informations exigées spécifiques à l'application et les détails de configuration nécessaires.

NOTE Si les appareils sont configurés avant leur arrivée sur site, il est préférable de réaliser la confirmation de leur configuration sur le site avant l'installation finale.

Les éléments d'entrée du processus de travail IDM pour l'acquisition de l'appareil intelligent doivent comprendre les éléments suivants:

- un programme IDM;
 - un plan de mise en œuvre de l'IDM;
 - un plan du projet de mise en œuvre de l'installation;
 - un calendrier du projet;
 - l'emplacement de l'appareil au sein de l'installation;
 - la liste des normes et spécifications du projet;
 - la liste des appareils à acquérir;
 - les certifications exigées;
- EXEMPLE Classement des zones électriques, et équipements spéciaux.
- la liste des emplacements fonctionnels et des identifications de tous les appareils;
 - les listes des types d'appareils agréés;
 - la liste de l'emplacement fonctionnel et de l'identificateur ultime (par exemple, le nom de l'étiquette) de tous les appareils;
 - la conformité aux normes de communication et d'échange d'informations diagnostiques.

Il convient que la phase d'acquisition ne débute pas tant que la liste des appareils à acquérir et les listes des types d'appareils agréés ne sont pas prêtes.

8.5.4.2 Spécification d'acquisition

Les exigences uniques concernant les appareils intelligents doivent comprendre les éléments suivants:

- document;
 - exigence de certification;
- NOTE La certification peut inclure l'électricité, la sécurité, les protocoles de communication et la cybersécurité.
- procédure de confirmation de l'exactitude du paramétrage au moment de l'expédition;
 - niveau de révision logicielle.

8.5.5 Préparation des données de configuration

8.5.5.1 Généralités

Il convient de définir le processus de travail IDM pour la préparation des données de configuration avant le début de la phase de conception et d'ingénierie. La préparation des données de configuration doit inclure un processus de vérification des données de configuration pour contrôler les critères de conception et l'application à l'appareil.

Le processus de travail IDM pour la préparation des données de configuration doit prendre en charge le ou les cas d'utilisation prévue par le concept de configuration pour la configuration des appareils intelligents pendant la phase initiale de construction et de mise en service de l'installation et la phase d'exploitation et de maintenance continue.

NOTE Les cas d'utilisation de la configuration peuvent inclure l'acquisition d'appareils intelligents configurés en usine et d'appareils intelligents configurés par des tiers, par exemple, des unités modulaires/hors site, différents scénarios de pré-mise en service/stockage sur site.

Au cours du processus de configuration, toute modification proposée doit faire l'objet d'une analyse d'impact afin de déterminer:

- l'étendue de cet impact sur les fonctions spécifiées de l'appareil intelligent;
- l'étendue des essais et de la vérification à réaliser ou à répéter concernant la modification proposée.

Le processus de configuration de l'IDM doit prévoir une prise en charge des aspects suivants:

- la future migration de la configuration de la révision de l'appareil;
- l'archivage de la configuration et la journalisation des révisions;
- la gestion de la maintenance, y compris la collecte de l'historique de maintenance.

Il convient que le processus de configuration de l'IDM prévoie la prise en charge des appareils intelligents d'accès à distance.

8.5.5.2 Éléments d'entrée et de sortie de la préparation des données de configuration

8.5.5.2.1 Généralités

Les éléments d'entrée du processus de travail IDM pour la préparation des données de configuration doivent comprendre les éléments suivants:

- objectifs du programme IDM;
- plan de mise en œuvre de l'IDM;
- plan du projet de mise en œuvre de l'installation;
- modèles d'appareil;
- spécification de configuration de chaque appareil.

Il convient que le point de départ de cette étape constitue le moment auquel les modèles d'appareil et la liste des appareils à configurer sont prêts.

Le résultat du processus de travail IDM pour la préparation des données de configuration doit prendre la forme d'ensembles de données de configuration dans une base de données de configuration pour chaque appareil intelligent individuel utilisé avec:

- un identificateur de rôle (numéro d'étiquette);
- un ensemble de paramètres à charger dans l'appareil intelligent;
- le modèle d'appareil utilisé pour l'élaboration des données de configuration;
- les informations relatives à la révision et à la date;
- le processus de vérification des données de configuration.

8.5.5.2.2 Modèles et typologies d'appareils intelligents

Les modèles d'appareils intelligents du fournisseur doivent comporter les informations suivantes:

- nom du modèle;
- description générale du type d'application (par exemple, pression, débit, niveau);
- ensemble de données de configuration;
- options de configuration.

Lors de l'élaboration des modèles d'appareil, il convient de prendre en considération la discontinuité du personnel, des outils, des processus et des procédures de travail.

Les modèles d'appareils doivent être maintenus pour refléter les changements apportés à chaque révision diffusée d'un appareil.

Il convient également de préparer des "typologies" de modèles pour les classes d'équipements fréquemment utilisées afin d'assurer la cohérence et d'améliorer l'efficacité de cette phase de conception et d'ingénierie.

NOTE Les "typologies" sont souvent fondées sur les modèles du fournisseur et sont généralement élaborées par l'utilisateur.

Le processus de conception et d'ingénierie doit tenir compte des changements apportés à la révision diffusée d'un appareil, soit par la prévention de toute modification après une certaine date ou un jalon important du projet (par exemple, la "date de gel"), soit par la mise à jour et le maintien continus des modèles d'appareils jusqu'à leur achèvement et leur transfert.

Il convient de préparer chaque ensemble de données de configuration d'un appareil intelligent sur la base du modèle d'appareil correspondant.

8.5.5.3 Gestion de configuration

8.5.5.3.1 Généralités

La gestion de configuration doit faire partie intégrante du programme IDM.

NOTE 1 Les processus de travail de la gestion de configuration peuvent être détenus et utilisés par les fournisseurs ou par les installations à différents moments.

La gestion de configuration de l'IDM doit inclure, au minimum, les éléments suivants:

- mise en œuvre;
- ressources;
- processus de travail; et
- formation/compétence.

La gestion de configuration doit:

- être conçue pour s'intégrer à l'IACS, au système de gestion de la maintenance et aux autres systèmes pertinents de l'installation;
- documenter la configuration détaillée agréée pour les appareils intelligents et les IACS connectés dans le cadre de l'installation pour la durée de vie de l'appareil intelligent.

La configuration agréée des appareils intelligents et des IACS connectés doit faire l'objet de pratiques de MOC fondées sur le classement par criticité de l'appareil intelligent.

Les spécifications des exigences fonctionnelles de l'appareil intelligent doivent être exprimées et structurées de telle manière qu'elles:

- soient claires, vérifiables et maintenues;
- facilitent la compréhension et l'interprétation des informations de toute phase du cycle de vie de l'installation IDM par les personnes qui les utilisent.

Il convient que la spécification des exigences d'application de l'appareil intelligent comprenne les exigences d'application issues du classement par criticité, notamment:

- les éléments à surveiller par classe d'équipement;
- la classification initiale et la priorité de chaque notification; et
- la politique d'escalade associée.

Les données de configuration doivent comprendre tous les paramètres de configuration de tous les appareils intelligents et tous les paramètres associés aux appareils intelligents de l'IACS.

NOTE 2 Ces paramètres de configuration peuvent être classés dans les catégories générales suivantes:

- paramètres de configuration associés aux fonctions de l'appareil intelligent;
- paramètres de configuration associés aux diagnostics de l'appareil intelligent;
- paramètres de configuration associés aux communications de l'appareil intelligent.

Les structures des messages d'intégration font partie de la gestion de configuration.

8.5.5.3.2 Mise en œuvre

Les pratiques de gestion de configuration de l'IDM doivent être documentées et communiquées aux participants de l'IDM pour la réalisation des activités IDM.

Il convient que le plan de mise en œuvre de la gestion de configuration établisse des étapes et des jalons spécifiques.

Le matériel et les logiciels nécessaires doivent être fournis pour effectuer les tâches de gestion de configuration et la documentation de leurs résultats.

Des ressources suffisantes et qualifiées doivent être régulièrement allouées pour vérifier que les tâches nécessaires peuvent être accomplies.

NOTE 1 Cette disposition exige un rapprochement des ressources et des actions pour combler tout manque de ressources identifié.

NOTE 2 Le classement par criticité des appareils intelligents constitue l'élément clé du rapprochement des ressources.

NOTE 3 La liste rapprochée des tâches reflète à la fois la réduction des risques et la création de valeur.

8.5.5.4 Base de données de configuration

Il convient que la base de données de configuration comprenne:

- un fichier de configuration de l'appareil – paramétrages d'un appareil intelligent et des bases de données associées;
- la configuration du système de commande;

NOTE 1 Le mode de réception et de transmission des données à d'autres systèmes tels que l'IHM, les automates et l'historique fait partie de la configuration de l'IACS.

NOTE 2 La configuration de l'IACS comprend également la manière dont le système réagit à différents types d'événements.

- la présentation de l'IHM – le mode et l'éventualité de la présentation des alarmes et alertes à l'opérateur ou à la personne appropriée pour une action corrective;
- les outils et les systèmes impliqués dans la gestion des appareils intelligents – quels paramètres doivent être transmis (directement ou indirectement) à des systèmes autres que le système de commande pour déclencher des actions correctives.

L'appareil intelligent et l'IACS connecté doivent être configurés pour répondre aux événements de diagnostic de l'appareil intelligent ou à toute autre détection de performances anormales dudit appareil, comme cela est spécifié dans l'application de l'appareil intelligent, y compris le classement par criticité associé.

NOTE 3 Les réponses spécifiées peuvent inclure la notification au personnel ou le traitement automatisé de l'IACS.

8.5.5.5 Spécification de configuration

La spécification de configuration des appareils intelligents doit déterminer et documenter, au minimum, les éléments suivants:

- la classification de la criticité des appareils intelligents (comme la sécurité, la commande, la cybersécurité, la qualité);

NOTE En fonction de la classification de la criticité, des normes supplémentaires peuvent s'appliquer. Par exemple, les appareils intelligents utilisés en SIS relèvent également du domaine d'application de la série IEC 61511.

- la justification de la classification des appareils;
- les fonctions des appareils intelligents qui doivent satisfaire aux exigences de l'application ou des applications prévues;
- l'interopérabilité des appareils intelligents;
- la réponse pour chacune des fonctions de l'appareil intelligent en cas de défaillance de ce dernier diagnostiquée en interne;
- l'interaction admise de l'opérateur ou du personnel de maintenance avec la ou les fonctions de l'appareil intelligent, y compris son fonctionnement manuel ou son contournement;
- les fonctions de sécurité souhaitées pour contrôler l'interaction locale ou à distance avec la ou les fonctions de l'appareil intelligent;
- les conditions de traitement qui permettent de soumettre à l'essai et de réparer en toute sécurité l'appareil intelligent en ligne.

Des procédures doivent être élaborées pour répondre à la détection d'une défaillance de l'appareil intelligent. Il convient que l'élaboration de la procédure prenne en considération les éléments suivants:

- quelles applications d'appareil intelligent exigent une procédure de réponse plus détaillée de l'appareil (par exemple, fondée sur la priorité ou la classe);
- les informations complémentaires à inclure dans les procédures de réponse de l'appareil intelligent (par exemple, cause, conséquence, action corrective);
- quelle méthode utilisée pour accéder aux procédures de réponse de l'appareil intelligent (par exemple, par le biais de l'interface humaine).

Des procédures doivent être élaborées pour répondre aux événements de diagnostic de l'appareil intelligent ou à toute autre détection de performances anormales dudit appareil. Il convient que l'élaboration de la procédure prenne en considération les éléments suivants:

- quelles applications d'appareil intelligent exigent une procédure de réponse plus détaillée de l'appareil (par exemple, fondée sur la priorité ou la classe);
- les informations complémentaires à inclure dans les procédures de réponse de l'appareil intelligent (par exemple, cause, conséquence, action corrective);
- quelle méthode utilisée pour accéder aux procédures de réponse de l'appareil intelligent (par exemple, par le biais de l'interface humaine).

8.5.5.6 Vérification des données de configuration

8.5.5.6.1 Généralités

Le processus de vérification des données de configuration doit être défini dans le cadre de la préparation des données de configuration afin de valider les critères de conception et l'application à l'appareil.

NOTE 1 Le processus de vérification peut être fondé sur un document et/ou une base de données, un essai de simulation ou une autre méthode.

Les critères de vérification doivent comprendre les révisions de l'appareil intelligent et des fichiers de support (EDD, DTM, etc.), l'exactitude, la conformité aux normes et les interfaces avec d'autres systèmes, ainsi que les valeurs des paramètres individuels.

Le processus de vérification des données de configuration doit tenir compte du concept de configuration utilisé pour le projet (usine, terrain, construction, combinaisons de ces éléments, etc.)

Il convient que le processus de vérification des données de configuration prenne en considération l'utilisation d'outils et de vérifications d'édition globale.

NOTE 2 Les outils d'édition globale ne sont pas nécessairement des outils réservés et peuvent constituer une fonction d'un autre logiciel de bureautique ou de gestion des actifs, ou une fonction mise en œuvre au moyen dudit logiciel. Les outils d'édition globale évitent tout transfert de paramètres individuels par l'automatisation ou la semi-automatisation de ce processus.

NOTE 3 Les vérifications d'édition globale peuvent également être utilisées lors de la phase d'exploitation et de maintenance pour contribuer à assurer la conformité continue de la configuration de l'appareil intelligent aux spécifications.

8.5.5.6.2 Spécifications des critères d'acceptation des appareils

Il convient d'utiliser les critères de choix des appareils intelligents comme la base des spécifications des critères d'acceptation. Les critères de choix à prendre en considération incluent les exigences spécifiées en matière de fonctionnalité de l'appareil intelligent et de l'IDM (telles que les notifications d'état et de diagnostic) nécessaires pour atteindre et maintenir les performances exigées de l'appareil intelligent et de l'IDM, en plus des exigences relatives aux fonctions primaires de l'appareil (par d'autres).

Les rapports d'essai de conformité aux normes pertinentes établis par des organismes tiers correspondants doivent être intégrés dans les critères d'acceptation des appareils.

EXEMPLE 1 Consortiums de bus de terrain responsables des organismes de certification des protocoles de communication.

EXEMPLE 2 Organismes de certification pour l'homologation électrique des zones dangereuses.

EXEMPLE 3 Certification de sécurité.

Les critères d'acceptation de l'appareil doivent également inclure la disponibilité générale des fichiers de support corrects de ce dernier (par exemple, EDD, FDI, DTM) par rapport aux spécifications et aux exigences de l'IACS.

8.5.6 Mise en œuvre et intégration des fonctions des appareils intelligents avec l'IACS

8.5.6.1 Généralités

La connectivité des appareils intelligents au système IDM est exigée.

Les appareils intelligents connectés par l'intermédiaire de l'IACS exigent des considérations spécifiques, comme cela est décrit dans les paragraphes suivants.

NOTE 1 D'autres interfaces d'appareils intelligents avec l'IACS peuvent exister en plus des connexions avec l'IACS, comme les appareils mobiles portatifs et les réseaux de communication des appareils intelligents réservés.

NOTE 2 Les exigences en matière de cybersécurité sont prises en considération pour chacune des différentes connexions IACS.

8.5.6.2 Architecture IACS

Il convient que la conception de l'architecture permette, dans la mesure du possible, un transfert "transparent" des données à l'intérieur et entre les couches pertinentes de l'IACS et du système de gestion des actifs associé.

NOTE Dans ce contexte, "transparent" signifie lisse et continu, sans écarts ou différences apparents entre les couches et les informations.

La conception de l'architecture IACS doit permettre l'accès à distance et/ou le support à distance selon les exigences de l'installation/entreprise. Il convient que la conception de l'architecture IACS prenne en considération l'assistance en nuage, y compris l'accès et l'hébergement des applications en nuage, dans le cadre de l'architecture de la solution.

La conception de l'architecture IACS doit prendre en considération la spécification des exigences fonctionnelles de l'application et les processus de travail IDM exigés.

Les exigences en matière d'opérabilité et de maintenabilité durables doivent être incluses dans la conception de l'architecture IACS.

L'architecture IACS doit intégrer au minimum les exigences en matière de cybersécurité du secteur dans lequel elle est déployée.

8.5.6.3 Interfaces IACS

La conception de l'interface IACS doit prendre en considération les exigences fonctionnelles de l'application de l'appareil intelligent et les processus de travail IDM définis, de sorte que les performances de communication de l'interface répondent aux spécifications du projet.

EXEMPLE Les performances des communications comprennent la disponibilité et les temps de réponse.

8.5.6.4 Fonctions de soutien au contrôle de l'IACS

Des procédures doivent être élaborées pour répondre à la défaillance d'un appareil intelligent détectée par l'IACS. Il convient que l'élaboration des procédures prenne en considération les éléments suivants:

- a) quelles applications d'appareil intelligent exigent une procédure de réponse plus détaillée de l'appareil (par exemple, fondée sur la priorité ou la classe);
- b) les informations complémentaires à inclure dans les procédures de réponse de l'appareil intelligent (par exemple, cause, conséquence, action corrective);
- c) quelle méthode utilisée pour accéder aux procédures de réponse de l'appareil intelligent (par exemple, par le biais de l'interface humaine).

Il convient que les procédures prévoient la prise en charge des appareils intelligents d'accès à distance.

8.5.6.5 Fonctions de soutien à la configuration de l'IACS

Voir 8.6.5 pour les considérations IACS concernant la migration de configuration des appareils intelligents.

8.5.6.6 IACS et sécurité des appareils

Il convient de préparer un ensemble de procédures de cybersécurité pour l'IACS et le système associé de gestion des actifs, par un alignement sur le programme global de cybersécurité de l'installation/entreprise.

NOTE De nombreux appareils intelligents ne comportent pas intrinsèquement d'outils de soutien à la cybersécurité. Le soutien à la cybersécurité de ces appareils repose sur des processus et procédures manuels et/ou des outils et appareils externes.

Il convient d'inclure les procédures dans le programme global de cybersécurité de l'installation/entreprise.

Les procédures de cybersécurité doivent être conformes aux normes de cybersécurité pertinentes, par exemple la série IEC 62443.

8.5.6.7 Fonctions de soutien sur le terrain de l'IACS

Les changements autorisés effectués localement sur l'appareil physique à l'aide d'outils indépendants de l'IACS (par exemple, ordinateur de poche, communicateur, calibre) doivent pouvoir être remis à jour dans l'IACS.

8.5.6.8 Prise en charge par l'IACS des exigences de maintenance et d'essai

L'IACS doit prendre en charge le niveau de disponibilité exigé pour l'essai de validation des appareils intelligents, l'essai fonctionnel et l'essai de validation.

La prise en charge IACS doit comprendre l'examen et l'essai manuels des appareils intelligents.

Il convient que l'IACS utilise le diagnostic des appareils intelligents pour réduire le plus possible les essais manuels.

8.5.7 Exigences en matière d'intégration et d'essai des systèmes

Les essais avec des appareils et des systèmes physiques classiques sur le terrain doivent être réalisés avant de générer des fichiers de configuration hors ligne globale qui seront utilisés dans les essais de configuration simulée.

NOTE 1 La génération des fichiers de configuration après leur vérification par essai réduit le plus possible toute reprise lors des activités ultérieures du cycle de vie.

Les configurations types doivent être préservées et reproduites pour une utilisation sur le terrain, ainsi que pour les ajouts, les modifications et les audits futurs en usine.

Les configurations types exigent une documentation d'accompagnement qui explique les choix effectués et les raisons de s'écarter de la configuration de modèle par défaut.

L'intégration et la configuration des systèmes nécessaires à l'assistance à l'IDM doivent être entièrement vérifiées par essai avant l'installation sur le terrain.

NOTE 2 Les essais hors site (comme le FAT) peuvent être et sont généralement réalisés à l'aide d'appareils de terrain simulés ou virtuels.

NOTE 3 Les essais assurent l'exhaustivité et l'exactitude des fichiers de configuration et des affichages IHM.

Les fichiers de configuration utilisés lors d'essais tels que le FAT doivent être conservés et utilisés sans modification jusqu'à l'installation sur site.

NOTE 4 De nombreux projets font référence à ce point comme un "point de gel".

NOTE 5 La conclusion de l'essai FAT a un système de fonctionnalité connue. Aucun changement n'intervient jusqu'à ce que le système soit réassemblé sur le site afin de disposer d'un point de départ stable pour la phase suivante du projet.

NOTE 6 Les projets passent à un autre système MOC à ce stade du projet et sont donc incapables de suivre ou de gérer les changements pendant le transfert.

Les exigences détaillées relatives à l'essai FAT doivent suivre l'IEC 62381.

Toutes les fonctions qui ne s'exécutent pas comme prévu pendant l'intégration sur le terrain et les changements qui en résultent doivent être validées par des essais formels et soigneusement documentés par le biais des processus MOC.

Le point de départ du MOC doit être fondé sur des configurations types vérifiées par essai et documentées par le FAT.

L'installation, l'intégration, la configuration et les essais finaux sur le site (y compris les SAT et SIT conformément à l'IEC 62381) doivent être terminés avant de commencer l'intégration des appareils de terrain et le contrôle de boucle (conformément à l'IEC 62382).

8.6 Construction et mise en service

8.6.1 Généralités

Les activités des phases précédentes du cycle de vie doivent être achevées comme cela est indiqué pour chaque activité de cette phase.

NOTE 1 Certaines activités, comme la mise en place du site et la construction, commencent généralement avant que toutes les activités de la phase d'ingénierie soient terminées.

Les processus de construction et de mise en service sont habituellement organisés selon une matrice d'attribution des responsabilités (RAM). La RAM doit décrire toutes les activités spécifiques à l'IDM à réaliser pendant la construction et la mise en service, ainsi que le rôle de chaque partie pour chaque activité individuelle.

L'état de chaque activité doit être suivi en même temps que l'état de la documentation et toutes les modifications techniques.

L'achèvement de la mise en service et de la revue de sécurité avant démarrage (PSSR) pour un groupe d'équipements dans une installation peut permettre l'exploitation de cet équipement alors que d'autres groupes d'équipements sont encore en construction et en mise en service.

La planification et la gestion de la construction et de la mise en service doivent permettre le chevauchement des phases du cycle de vie, le cas échéant.

NOTE 2 Des procédures supplémentaires d'autorisation et de gestion sont généralement nécessaires lorsque les activités de construction et de mise en service sont menées dans une installation en exploitation ou lorsqu'elles peuvent avoir un impact sur une installation en exploitation.

Le travail sur le terrain doit être programmé à l'avance et inclure la séquence des activités à effectuer, les rôles et les responsabilités, ainsi que des plans détaillés et spécifiques d'exécution des activités.

L'Article 8 couvre une séquence d'activités. L'ordre suivant de la séquence doit être fourni pour chaque groupe d'équipements afin d'assurer l'intégrité des résultats:

- a) mise en place du site (tout le travail de préinstallation);
 - 1) identification et stock;
 - 2) pièces de rechange;
- b) installation;
 - 1) vérification du câblage et mise sous tension;
- c) approvisionnement;
- d) configuration;
- e) contrôle de boucle et mise en service;
 - 1) formation du personnel;
 - 2) exploitation des outils de production et application des procédures d'essai;
 - 3) en service et prêt à démarrer;
- f) transfert;
 - 1) documentation (en l'état de fabrication, balisages, etc.);
 - 2) responsabilité de la maintenance;
- g) PSSR.

8.6.2 Mise en place du site

Pendant les activités sur le site, il convient que la première activité consiste à vérifier que l'équipement reçu correspond aux spécifications d'acquisition.

Les éléments individuels de l'équipement doivent être étiquetés de façon permanente.

Les pièces de rechange doivent être identifiées par type d'équipement et étiquetées comme telles.

Il convient de stocker les pièces de rechange séparément du stock étiqueté ou attribué.

Le stockage de l'équipement doit protéger son intégrité.

Les activités facultatives comprennent un essai en atelier.

NOTE L'essai en atelier peut comprendre: configuration de l'appareil, contrôle de fonctionnement, vérification d'étalonnage, etc.

8.6.3 Installation

L'ordre d'installation suit le plan de construction du site.

L'installation de l'appareil intelligent doit être conforme à la conception détaillée et à la spécification des exigences.

Il convient que les modifications d'installation de l'appareil intelligent suivent le processus MOC. Il convient que la documentation comporte, entre autres: les plans d'implantation, les plans de construction, les plans de raccordement, le manuel et les plans d'installation du fabricant de l'équipement et les plans du réseau.

NOTE 1 Il existe des lignes directrices officielles d'installation et de mise en service préparées par des organisations telles que les organisations de bus de terrain, qui servent de lignes directrices destinées à assurer une installation correcte des appareils intelligents (par exemple, lignes directrices spécifiques au protocole).

L'installation de l'appareil intelligent doit suivre les bonnes pratiques d'installation.

Le câble de communication des appareils intelligents et la mise à la terre doivent être effectués en respectant strictement les documents d'ingénierie.

NOTE 2 Une formation de l'équipe d'installation sur le terrain aux pratiques de câblage des instruments est souvent exigée pour assurer le respect des exigences techniques.

EXEMPLE Séparation des câbles de signaux et d'alimentation, par exemple en évitant de faire passer les câbles de signaux le long des câbles d'alimentation et en utilisant des presse-étoupes CEM.

8.6.4 Approvisionnement

Cette activité doit être lancée après la mise à disposition des informations exigées relatives à l'ingénierie, la documentation, l'installation et la mise en œuvre du système.

NOTE 1 Cette activité constitue le début de la configuration finale et de la mise en service et ne peut être réalisée qu'avec un support système complet et une ingénierie achevée.

NOTE 2 Cette activité fournit une application et un appareil avec les identités nécessaires pour terminer la configuration et la mise en service.

NOTE 3 Cette activité comprend l'adhésion au réseau de communication sur le terrain et permet une communication sécurisée avec les systèmes si nécessaire.

Une procédure d'approvisionnement formelle doit être utilisée pour confirmer l'identité de l'application et de l'appareil, y compris l'étiquetage physique et logiciel et l'installation au bon emplacement.

L'approvisionnement doit inclure une confirmation manuelle par le personnel sur le terrain.

L'approvisionnement doit être achevé avant les étapes suivantes telles que la configuration, le contrôle de boucle et la mise en service.

L'achèvement de l'approvisionnement peut déclencher automatiquement le téléchargement de la configuration.

8.6.5 Configuration

Il convient de prévoir pour la configuration des procédures de téléchargement de paramètres à partir d'une base de données prévérifiée.

La saisie manuelle des données de la configuration des appareils intelligents doit être complétée par des procédures supplémentaires qui permettent de vérifier l'intégrité des données saisies.

NOTE 1 La saisie manuelle des données est source d'erreurs et ne constitue pas la procédure de configuration préférentielle. Le téléchargement automatisé est préférable dans la mesure du possible.

La configuration de l'appareil intelligent doit être sauvegardée, et les fichiers de sauvegarde doivent porter la mention "Tel qu'installé" afin de conserver toute modification future de la configuration pendant la mise en service sous forme de dossier.

NOTE 2 Les appareils intelligents comportent souvent des centaines de paramètres configurables.

Les outils et les processus de travail pour la configuration de l'appareil intelligent et la gestion des notifications doivent être achevés à temps pour pouvoir utiliser les diagnostics de l'appareil intelligent pendant le contrôle de boucle.

Il convient que l'utilisation initiale des outils et procédures serve à la formation du personnel.

Tous les appareils intelligents pertinents correctement configurés et les dossiers relatifs au travail de configuration doivent constituer le résultat du processus de travail IDM de configuration.

Un rapport d'installation complet doit être généré par appareil intelligent.

Le rapport d'installation de l'appareil intelligent doit indiquer l'état de celui-ci et l'index des appareils intelligents doit également être mis à jour.

L'index des appareils intelligents et les rapports sur lesdits appareils doivent être remis à l'équipe de mise en service de manière à fournir des recommandations pour la préparation du plan de mise en service.

8.6.6 Contrôle de boucle et mise en service

Les essais SAT et SIT doivent être réalisés avant d'effectuer les contrôles de boucle.

NOTE 1 Les SAT et SIT sont traités dans l'IEC 62381.

Le contrôle de boucle doit commencer par la vérification et l'approbation de l'installation, de l'approvisionnement et de la configuration pour vérifier que toutes les dispositions de la conception technique ont été correctement mises en œuvre.

Un contrôle de fonctionnement de boucle doit ensuite être effectué pour vérifier que les appareils et les systèmes sont correctement intégrés et fonctionnent comme prévu.

NOTE 2 Le contrôle de fonctionnement de boucle comprend la vérification des plages d'instruments dans les appareils et les systèmes.

Le contrôle de fonctionnement de boucle doit inclure l'exercice de toutes les procédures d'essai formelles préparées pour le soutien à long terme des installations.

Le contrôle de fonctionnement de boucle doit être achevé et approuvé avant de commencer les activités de mise en service de l'appareil.

Les procédures de mise en service doivent être formelles et comprendre toutes les procédures exigées pour la mise en service des appareils et des boucles.

Les procédures de mise en service doivent inclure des activités et des essais tels que le réchauffage des conduites, les systèmes d'échantillonnage, les vannes de coupure de procédé, les tubes de remplissage, ou d'autres vérifications ou essais finaux si nécessaire.

Certaines procédures de mise en service (comme les systèmes d'échantillonnage) peuvent dépendre de l'état de préparation du processus et peuvent exiger un report jusqu'à un moment approprié.

Toute anomalie dans l'installation ou la documentation doit être corrigée avant approbation.

Une approbation formelle de la mise en service doit être exigée. Cette approbation doit indiquer l'achèvement des activités de construction et la préparation des appareils, des systèmes et de la documentation pour la PSSR et le transfert vers l'exploitation et la maintenance.

Les procédures de mise en service de l'IDM doivent être achevées et les anomalies identifiées doivent être résolues avant la PSSR (ou une activité équivalente avant la fin du démarrage d'une installation).

Il convient de considérer la participation au contrôle de fonctionnement de boucle et à la mise en service comme un exercice de formation pour le personnel de l'installation.

Il convient d'éviter les lacunes de couverture entre le personnel des phases de construction et de mise en service et le personnel d'assistance à long terme.

NOTE 3 Se reporter à l'IEC 62382 pour le contrôle de boucle.

Il convient de préparer le plan de mise en service avant que la configuration des appareils intelligents concernés soit terminée.

Il convient que le plan de mise en service prenne en considération les activités suivantes:

- a) vérification de l'installation et de l'étiquetage pour assurer que le bon appareil est installé au bon emplacement;
- b) établissement d'une communication numérique avec l'IACS;
- c) téléchargement des paramètres (en amont et en aval) qui permettent d'assurer la synchronisation des bases de données (sauvegardes, etc.) en fonction de la procédure de configuration effectivement utilisée;
- d) réalisation d'un essai d'intégration et d'un essai fonctionnel, par exemple des essais en boucle, afin de vérifier que les fonctions s'exécutent comme prévu selon la version autorisée, y compris les alertes de diagnostic vérifiables par essai;
- e) transfert entre le contrôle des modifications de conception et le contrôle des modifications d'exploitation;
- f) installation finale pour que l'appareil soit prêt à fonctionner;
- g) vérification de l'étalonnage (c'est-à-dire le zéro, la plage, l'étendue, etc.);
- h) évaluation afin d'assurer l'état de préparation opérationnelle.

Tous les appareils intelligents pertinents vérifiés pour les applications prévues et les dossiers relatifs au travail de mise en service doivent constituer le résultat du processus de travail IDM de mise en service. Les enregistrements de l'appareil intelligent, y compris la configuration, les réglages et les essais réalisés, doivent être conservés avec les enregistrements de la boucle associée.

8.6.7 Formation et compétence du personnel

Le personnel qui effectue le travail doit être formé aux processus, procédures et tâches qui lui sont assignés.

Un système de suivi des compétences par rôle et par personnel doit être mis en place.

Les exigences d'un programme de formation durable comprennent les éléments suivants:

- évaluation des compétences des travailleurs et des lacunes en matière de compétences;
- acquisition des compétences nécessaires;
- revue et mise à jour périodiques des programmes de formation; et
- revue de la formation exigée pour les nouveaux appareils intelligents, y compris, entre autres, les processus et les procédures de travail, ainsi que les tâches.

Il convient que la formation comprenne la familiarisation avec l'équipement, les outils utilisés pour travailler avec l'équipement, ainsi que les techniques et les normes spécifiques ou les modèles d'application des appareils utilisés dans l'installation.

Il convient que la formation à l'utilisation du système IDM du personnel impliqué dans les phases d'exploitation et de maintenance commence avant, ou pendant, la mise en service afin de le familiariser avec les nouveaux outils.

Il convient que la formation du personnel à l'IDM soit terminée à temps pour utiliser les diagnostics pendant l'installation et le contrôle de boucle. La formation doit également être terminée avant le transfert.

NOTE La formation peut être menée séparément du contrôle de boucle et de la mise en service, ou bien elle peut être combinée à ces activités.

Les compétences exigées des individus en matière de dépannage doivent être définies avant la phase d'exploitation et de maintenance du projet.

Il convient de réaliser une formation et une évaluation des compétences avant la PSSR.

8.6.8 Transfert

Il convient de documenter toutes les informations pertinentes sur l'ingénierie IDM et les appareils des fournisseurs au fur et à mesure qu'elles sont générées. Il convient de prévoir un accès à ces informations en temps utile aux personnes en fonction de leurs responsabilités.

Des processus et des outils de travail doivent être préparés pour gérer la phase de transfert du cycle de vie de l'installation IDM.

La documentation et les autres informations exigées doivent être fournies dans un format auquel le personnel du site peut accéder et qu'il peut utiliser et conserver.

Une installation doit comporter des plans d'accès, d'utilisation et de conservation des informations après le transfert.

8.6.9 PSSR

Tous les outils, processus de travail et procédures de maintenance, ainsi que la formation et les ressources en personnel doivent être en place préalablement à la PSSR (ou une activité équivalente) avant le démarrage d'une installation.

Toutes les listes de contrôle doivent être complètes, et les procédures doivent être vérifiées par essai et approuvées avant la PSSR.

NOTE 1 La PSSR peut être complétée pour chaque groupe d'équipements dans une installation prête à être mise en service.

NOTE 2 La réalisation de la PSSR assure qu'un groupe d'équipements est prêt à fonctionner.

8.6.10 Démarrage

Des procédures IDM formelles doivent être établies et mises en œuvre pour la phase de démarrage du cycle de vie d'une installation.

NOTE 1 Le démarrage introduit des dangers potentiels qui peuvent être différents des dangers des phases précédentes du cycle de vie. Les différences portent sur les différents types de dangers et la gravité des conséquences.

NOTE 2 Les méthodes utilisées pour gérer le risque opérationnel sont différentes de celles utilisées pour les phases précédentes du cycle de vie. La gestion du risque opérationnel est active pendant le démarrage.

Lorsque le démarrage est progressif ou séquentiel, des procédures supplémentaires de sécurité et de gestion des données doivent être mises en place pour gérer les activités simultanées de construction et d'exploitation.

NOTE 3 La construction et l'exploitation simultanées exigent généralement des outils et des procédures supplémentaires pour empêcher les systèmes de gestion de la construction et de l'exploitation d'interférer entre eux.

8.7 Exploitation et maintenance

8.7.1 Généralités

Avant d'entrer dans la phase d'exploitation et de maintenance du cycle de vie de l'installation, des outils, des ressources, des processus de travail et des procédures nécessaires doivent être fournis pour maintenir la fonctionnalité spécifiée de l'application de l'appareil intelligent et les exigences globales de performances de l'IDM d'une manière conforme aux exigences du programme IDM.

Il convient que la préparation des outils, ressources, processus de travail, et procédures ci-dessus prenne en considération chaque application individuelle de l'appareil intelligent.

Les processus de travail IDM suivants doivent au minimum être définis pour les activités IDM exécutées dans cette phase du cycle de vie de l'installation sur la base du programme IDM:

- a) processus de prépréparation;
- b) processus de réparation (y compris le remplacement et la gestion des stocks);
- c) processus de post-réparation;
- d) processus de gestion des stocks.

NOTE Les dispositions relatives à ces processus de travail IDM sont spécifiées dans les paragraphes suivants.

Il convient de contrôler, évaluer et améliorer le processus de travail IDM en permanence à l'aide du processus de travail de MOC.

Il convient que le processus MOC prenne en charge et gère les modifications de conception de l'installation (qu'il s'agisse d'une mise à niveau complète du système de commande et du logiciel ou du remplacement d'un appareil mineur) pendant l'exploitation de cette dernière.

Il convient de choisir les types appropriés de processus de maintenance et de les appliquer à chaque appareil intelligent sur la base d'une détermination de la criticité.

NOTE Les types de processus de maintenance comprennent:

- l'exploitation jusqu'à défaillance;
- la maintenance fondée sur le diagnostic;
- le traitement automatisé des pannes;
- les examens et les essais prévus.

Les processus de travail de maintenance doivent être préparés sur la base du programme IDM.

L'historique de maintenance doit être collecté afin d'analyser les données qui en résultent pour dégager des tendances, des améliorations et des mesures qui permettent de déterminer l'efficacité du programme de maintenance choisi qui est mis en œuvre.

Les activités de maintenance doivent documenter l'état de l'équipement (observé), et mentionner si des réparations de suivi sont nécessaires.

8.7.2 Processus de surveillance continue des appareils intelligents, et processus d'identification et de diagnostic des problèmes

8.7.2.1 Dispositif de surveillance des appareils intelligents

Les informations sur les paramètres d'état et de condition qui sont exigées par la configuration spécifiée pour l'application de l'appareil intelligent doivent être collectées et conservées conformément au programme IDM et à l'application d'utilisation de ce même appareil.

Il convient que la collecte et la conservation des informations du dispositif de surveillance des appareils soient réalisées de manière automatique et continue, éventuellement par une surveillance à distance.

Il convient de prendre en considération l'accès à distance aux appareils intelligents pour les essais desdits appareils avec des appareils IHM locaux.

Il convient que les messages de diagnostic des appareils intelligents fassent l'objet d'un enregistrement automatique. S'il est réalisé par l'intermédiaire du système de communication IACS, l'appareil intelligent doit être configuré pour répondre aux demandes de renseignements ou pour transmettre des informations sur son état.

Il convient que des outils de consignation à degré normal de capacité d'analyse transmettent des informations sur le dispositif de surveillance des appareils.

Il convient de définir des processus et procédures de travail pour la personne responsable ayant l'autorité de répondre et d'agir sur les informations de surveillance, en fonction du classement par criticité et des paramètres du type d'appareil à surveiller.

Il convient que le fournisseur de l'appareil spécifie la couverture de diagnostic de l'appareil intelligent et confirme quels diagnostics sont effectivement couverts, en particulier pour les mises en œuvre de sécurité dans la mesure où ce paramètre influence les calculs SIL.

Il convient également de contrôler l'intégrité de la configuration des appareils intelligents.

Le programme IDM doit établir un système de surveillance des performances des appareils intelligents.

L'entreprise doit identifier et mettre en œuvre les exigences relatives à la communication et à la gestion des notifications des appareils intelligents concernant leur diagnostic, telles qu'elles sont définies dans le programme IDM.

NOTE 1 La communication et la gestion des notifications de diagnostic des appareils intelligents peuvent être différentes pour un même type d'appareil, selon l'importance de la fonction de ce dernier et l'impact du diagnostic sur l'appareil.

NOTE 2 Se reporter à la Figure 18 de l'IEC TR 63082-1:2020.

8.7.2.2 Essais fonctionnels et examen des appareils intelligents

Les processus et procédures de travail IDM doivent prendre en charge les exigences d'examen et d'essai spécifiées pour l'application qui utilise l'appareil intelligent.

Les essais doivent également inclure des essais d'entrée de processus pour vérifier la fonctionnalité complète plutôt que la seule fonction de communication.

Les enregistrements, les résultats et la documentation relatifs aux essais fonctionnels et à l'examen des appareils intelligents doivent être conservés et stockés par l'installation. La conservation des enregistrements et de la documentation doit être définie par l'entreprise.

8.7.2.3 Étude des problèmes relatifs aux appareils intelligents

Des processus et des procédures de travail pour l'étude des problèmes relatifs aux appareils intelligents doivent être développés. Il convient que ces processus et procédures comportent des mesures à surveiller pour détecter les problèmes qui exigent une enquête plus approfondie pour identifier les symptômes.

Les processus d'étalonnage, de réparation ou de remplacement doivent être déclenchés lorsque l'étude identifie les travaux exigés.

8.7.3 Étalonnage des appareils intelligents

Un processus de travail pour l'étalonnage doit être développé en fonction des types d'appareils et de la technologie.

Il convient de considérer l'étalonnage semi-automatique utilisant la fonction de réglage supplémentaire des appareils intelligents comme un outil d'étalonnage desdits appareils avec une source de signal de référence par l'intermédiaire du réseau.

Il convient de considérer l'enregistrement semi-automatique des travaux d'étalonnage utilisant la capacité de communication des appareils intelligents comme un outil d'étalonnage desdits appareils avec une source de signal de référence par l'intermédiaire du réseau.

L'étalonnage doit également inclure des essais d'entrée de processus pour vérifier la fonctionnalité complète plutôt que la seule fonction de communication.

8.7.4 Processus de réparation

8.7.4.1 Généralités

Les défaillances identifiées de l'appareil intelligent ou les dégradations révélées doivent être corrigées dans les délais prévus pour l'application spécifique de l'appareil. En l'absence d'application spécifique de l'appareil intelligent, la réparation ou le remplacement de l'appareil doit être conforme à son classement par criticité.

L'exécution de la réparation ou du remplacement de l'appareil intelligent doit être enregistrée sur la base des lignes directrices de l'installation aux fins suivantes:

- planification de la maintenance;
- analyse de fiabilité;
- contrôle des stocks.

8.7.4.2 Réparation de boucle

Le processus de travail pour la réparation de boucle doit être déterminé en fonction des lignes directrices de l'installation pour ramener la boucle à sa fonction d'origine.

Le processus de travail pour la réparation de boucle peut comprendre les éléments suivants:

- consignation de l'état de l'appareil;
- notification de l'état de l'appareil à l'opérateur;
- confirmation par l'opérateur de l'état de l'appareil et de l'impact sur le processus;
- signification par l'opérateur de l'état de l'appareil au personnel de maintenance;
- réalisation du dépannage initial par la maintenance de l'appareil intelligent;
- réparation en ligne ou hors ligne de l'appareil;
- remise de l'appareil en état de fonctionnement.

La réparation de boucle doit être initiée lorsque des défaillances ou des dégradations d'une boucle sont détectées.

NOTE 1 Les défaillances et les dégradations des boucles peuvent être détectées par la surveillance, l'étalonnage, l'examen et le diagnostic de l'appareil.

Pour identifier la cause de la défaillance ou de la dégradation, il convient d'effectuer une recherche des causes, comme le dépannage.

Pour choisir un processus de réparation adapté à la situation, il convient de déterminer les risques de laisser la boucle en l'état et les impacts de la réparation.

Un processus de réparation doit être choisi en fonction de la cause identifiée et du résultat de l'analyse des risques et des impacts.

NOTE 2 Les processus de réparation potentiels comprennent le changement de configuration du système hôte, le changement de configuration de l'appareil intelligent, la mise à niveau du micrologiciel de l'appareil intelligent, la réparation des connexions et le remplacement de l'appareil intelligent.

Le cas échéant, la réparation peut être reportée jusqu'à la prochaine révision. Dans ce cas, des informations suffisantes doivent être communiquées à l'équipe pour la planification de ladite révision.

La procédure de chaque type de processus de réparation doit être documentée sur la base du programme IDM et des lignes directrices de l'installation.

NOTE 3 Certaines exigences et recommandations pour l'élaboration des procédures des types de processus de réparation sont spécifiées dans les paragraphes suivants.

La réparation de la boucle sélectionnée doit être exécutée en suivant sa procédure.

Après réalisation de la réparation, un essai de vérification de l'appareil doit être effectué pour confirmer que celle-ci a été correctement effectuée. En cas d'échec de l'essai de vérification de l'appareil, la réparation doit être effectuée à nouveau.

Après l'essai de vérification de l'appareil, un essai de validation de boucle doit être exécuté pour confirmer que la boucle peut fonctionner correctement. En cas d'échec de l'essai de validation de boucle, la réparation doit être effectuée à nouveau.

8.7.4.3 Réparation des appareils intelligents

8.7.4.3.1 Réparation du matériel des appareils intelligents

Le processus de travail doit être déterminé en fonction des lignes directrices de l'installation propres à la réparation de l'appareil. La réparation peut être effectuée sur site ou hors site.

- Il convient que la réparation sur site suive les recommandations du fabricant.
- Il convient que la réparation hors site soit effectuée par un centre de réparation certifié par le fabricant.

8.7.4.3.2 Reconfiguration des appareils intelligents

Les données de configuration de chaque appareil intelligent doivent être conservées et mises à jour.

Les données de configuration de l'appareil intelligent doivent être déterminées pendant la phase d'ingénierie et de conception et doivent être communiquées par le système hôte. La documentation technique doit être conservée et confirmée dans le système hôte.

La reconfiguration d'un appareil intelligent doit être mise en œuvre lorsqu'une modification des données de configuration est convenue au niveau de l'installation qui détermine qu'une configuration différente est exigée.

En vue de la reconfiguration d'un appareil intelligent, l'installation doit élaborer une stratégie de mise en œuvre comprenant des modèles, des outils, des essais, des revues de procédures, des exigences IACS et de la documentation.

Il convient de considérer la configuration à distance qui utilise la capacité de communication des appareils intelligents comme un outil de reconfiguration desdits appareils.

NOTE La modification des conditions du processus ou de la maintenance peut également affecter les paramètres de diagnostic de maintenance.

Il convient d'effectuer la sauvegarde et la restauration des données régulièrement avec un archivage sécurisé selon les bonnes pratiques.

La reconfiguration des appareils intelligents doit suivre la procédure MOC.

8.7.4.3.3 Mise à niveau de micrologiciel des appareils intelligents

La ou les mises à niveau de micrologiciel de chaque appareil intelligent doivent être évaluées avant mise en œuvre.

NOTE 1 Une mise à niveau du micrologiciel peut avoir un impact involontaire sur les performances d'un appareil intelligent dans une boucle. La vérification par essai d'une mise à niveau de micrologiciel avant sa mise en œuvre peut être considérée comme une partie intégrante de l'évaluation. La vérification par essai de la boucle après une mise à niveau du micrologiciel pour confirmer le bon fonctionnement peut également être prise en considération.

La mise à niveau du micrologiciel d'un appareil intelligent doit être exécutée par une procédure fondée sur la version du fabricant du micrologiciel pour un appareil intelligent existant.

Il convient de considérer la mise à niveau en ligne du micrologiciel comme un outil de reconfiguration des appareils intelligents.

Il convient d'enregistrer les raisons et les résultats de la mise à niveau du micrologiciel.

La MOC par type d'appareil plutôt que par application lors de la mise à niveau vers une nouvelle révision du micrologiciel doit être prise en considération.

NOTE 2 Comme l'appareil en cours de mise à niveau n'est pas disponible pendant cette opération, le processus peut être affecté, ce qui peut exiger des procédures de remise en service pour redémarrer.

8.7.5 Remplacement des appareils intelligents

8.7.5.1 Généralités

Il doit être confirmé au préalable, pendant l'évaluation et avant le remplacement que toutes les fonctions utilisées de l'appareil intelligent installé sont couvertes par l'appareil de remplacement. Dans le cas où des fonctions supplémentaires (par exemple, la fonction de diagnostic et la fonction de mesure multivariable) sont utilisées, leurs informations détaillées fonctionnelles doivent être conservées après le remplacement.

En outre, l'interopérabilité entre les systèmes hôtes et l'appareil intelligent de remplacement doit être évaluée et maintenue. Il convient d'utiliser le résultat de l'essai d'interopérabilité fourni par le fabricant de l'appareil intelligent comme un élément de l'évaluation de l'interopérabilité entre les systèmes hôtes et l'appareil intelligent, s'il est disponible.

8.7.5.2 Ingénierie de remplacement des appareils intelligents

Lorsque le fabricant de l'appareil intelligent notifie un changement relatif à ce dernier, les impacts de la modification de conception doivent être évalués.

NOTE 1 Les changements relatifs aux appareils intelligents peuvent être la mise à niveau du micrologiciel, la mise à jour de la version ou l'obsolescence du modèle de l'appareil intelligent. Un modèle d'appareil intelligent similaire du même fabricant, un modèle d'appareil intelligent similaire d'un fabricant différent, ou un modèle d'appareil intelligent fondé sur une technologie différente peuvent constituer des solutions alternatives à l'obsolescence par le fabricant.

Sur la base de l'analyse de l'impact du changement proposé, les changements relatifs à un appareil intelligent installé doivent être gérés conformément aux exigences du programme IDM en matière de MOC et aux pratiques et procédures MOC relatives à l'application ou aux applications dans lesquelles l'appareil intelligent est utilisé.

L'évaluation des modifications de conception doit être effectuée selon une procédure d'évaluation appropriée en fonction du type de modification de conception.

L'évaluation doit vérifier la fonctionnalité de tout nouveau type d'appareil par rapport aux exigences relatives à chaque utilisation de l'appareil installé en matière de logiciel et de matériel.

L'évaluation et les essais doivent déterminer si les variations des changements de configuration et des options sont acceptables et si de nouvelles fonctionnalités doivent être utilisées.

Des procédures d'évaluation documentées pour chaque type de changement doivent être fournies à l'avance selon les paragraphes suivants du présent document comme partie intégrante du programme IDM. Il convient qu'elles fassent l'objet d'une revue et d'une mise à jour régulières.

Les problèmes éventuels de compatibilité constatés au cours de l'évaluation doivent être résolus.

NOTE 2 La solution peut être la modification des données de configuration de l'appareil intelligent ou les modifications des systèmes hôtes, y compris la modification du programme d'application.

En fonction du résultat de l'analyse documentaire fondée sur les fiches de spécifications des appareils intelligents et de la procédure d'évaluation, des essais sur des échantillons d'appareils intelligents doivent être réalisés.

NOTE 3 L'analyse documentaire détermine si une appréciation du risque est exigée.

Si l'évaluation conclut que la modification de conception n'est pas acceptable, il convient de demander au fabricant des propositions de solutions alternatives.

Si l'évaluation conclut que la modification de conception est acceptable, des procédures documentées de remplacement de l'appareil intelligent doivent être élaborées sur la base des lignes directrices de l'installation.

Les procédures de remplacement des appareils intelligents doivent suivre le processus MOC de l'installation.

Le résultat d'évaluation doit être documenté.

La documentation relative à la dernière révision du matériel, du micrologiciel, du logiciel intégré et des paramètres de configuration de l'appareil intelligent agréé doit être conservée.

NOTE 4 Cette information est essentielle pour réaliser la MOC des appareils intelligents.

Les procédures de remplacement en matière de compatibilité des modèles pour chaque combinaison possible d'appareil intelligent installé et d'appareil intelligent de remplacement doivent être fournies.

NOTE 5 Les combinaisons possibles entre l'appareil intelligent installé et l'appareil intelligent de remplacement peuvent être le remplacement par le même modèle avec la même version, le remplacement par le même modèle avec une version différente, le remplacement par un modèle différent du même fabricant, le remplacement par un modèle d'un fabricant différent ou le remplacement par un modèle fondé sur une technologie différente.

Les procédures de remplacement doivent tenir compte des modifications des données de configuration de l'appareil intelligent et des systèmes hôtes, y compris les logiciels d'application.

Il convient d'utiliser des outils de support à la migration semi-automatique/automatisée lors du changement de révision des appareils.

NOTE 6 Chaque option de remplacement/changement devient de plus en plus complexe et exige une MOC supplémentaire.

Les procédures de remplacement doivent faire l'objet d'une revue et d'une mise à jour régulières.

Les changements ou modifications apportés à l'appareil intelligent doivent être documentés et archivés.

NOTE 7 Il est nécessaire de saisir les modifications dans les outils de conception et de les traiter en fonction de la nouvelle configuration en vue d'un enregistrement direct des mises à jour des modifications après réalisation.

NOTE 8 Si la procédure relative à un appareil intelligent en l'état est applicable, elle est incluse dans le processus de changement.

8.7.5.3 Remplacement en nature de l'appareil intelligent

Avant d'effectuer le remplacement en nature de l'appareil intelligent, les éléments suivants doivent être vérifiés:

- les spécifications de modèle et de matériel de l'appareil de remplacement sont maintenues identiques à celles de l'appareil installé;
- la révision du micrologiciel et la révision des outils utilisables (par exemple, le fichier EDD) de l'appareil intelligent de remplacement sont les mêmes que celles de l'appareil installé; et
- les paramètres de configuration de l'appareil de remplacement sont maintenus identiques à ceux de l'appareil installé.

NOTE Les paramètres de configuration peuvent être téléchargés dans l'appareil de remplacement par le système hôte.

8.7.5.4 Remplacement de l'appareil intelligent par un micrologiciel révisé

La procédure d'évaluation appropriée doit être déclenchée lorsqu'une version révisée du micrologiciel d'un appareil intelligent est diffusée afin de déterminer l'impact des changements opérés et si un remplacement sera mis en œuvre.

La procédure d'évaluation du micrologiciel révisé doit:

- confirmer que la fonctionnalité de l'appareil de remplacement est compatible avec l'appareil installé;
- définir les procédures exigées pour remplacer, le cas échéant, l'appareil intelligent actuel par une version révisée du micrologiciel en suivant les lignes directrices du fabricant;
- identifier les paramètres de configuration à définir sur l'appareil de remplacement;
- identifier les mises à jour logicielles, les paramètres de configuration et les données à définir sur les systèmes hôtes;
- déterminer s'il est nécessaire de procéder à des essais avant le remplacement et définir la procédure d'essai, le cas échéant;
- définir les procédures d'essai après le remplacement, y compris l'exploitabilité de l'appareil et son intégration au système hôte, ainsi que la vérification par essai de la boucle associée.

8.7.5.5 Remplacement de l'appareil intelligent par un modèle différent

Dans le cas où le fabricant d'un type d'appareils installés développe un modèle différent qui est un remplacement direct de l'appareil installé, chaque appareil installé peut être remplacé par un appareil du modèle différent.

8.7.5.6 Remplacement de l'appareil intelligent par un autre fabricant

Dans le cas où le fabricant d'un type d'appareil installé n'est pas en mesure de continuer à fournir un remplacement direct, il convient de trouver un appareil de remplacement auprès d'un autre fabricant.

Le fabricant de l'appareil de remplacement doit être évalué (par exemple, performances, formation, outils d'essai, protocole de fabrication, pièces de rechange).

8.7.5.7 Remplacement de l'appareil intelligent par une technologie différente

Avant de remplacer un appareil intelligent par une technologie différente, la MOC doit vérifier que le domaine d'application fonctionnel initial est couvert.

NOTE Dans ce contexte, une technologie différente signifie un changement dans la technologie de détection des appareils de terrain.

8.7.5.8 Exécution de remplacement des appareils intelligents

Il convient de prendre en considération le remplacement d'un appareil intelligent si la réparation de l'appareil ou de la boucle en ligne n'est pas acceptable.

Le remplacement d'un appareil intelligent doit être effectué selon la procédure appropriée en fonction de la situation de compatibilité.

NOTE 1 Les situations de compatibilité comprennent le même modèle avec la même version, le même modèle avec une version différente, un modèle différent du même fabricant, un modèle différent d'un fabricant différent et un appareil fondé sur une nouvelle technologie.

Les paramètres de configuration de l'appareil de remplacement doivent être réglés de manière correcte selon la procédure de remplacement.

Les paramètres des systèmes hôtes liés à l'appareil doivent être reconfigurés selon la procédure de remplacement.

Après le remplacement, un essai de vérification de l'appareil doit être effectué.

Un essai de validation de la boucle doit être exécuté selon les lignes directrices de l'installation, avec mise en exergue de la partie de la boucle qui a été remplacée.

Le résultat du remplacement doit être enregistré dans les dossiers de maintenance après son achèvement.

Un dossier des activités de travail doit être créé chaque fois qu'une activité de maintenance est effectuée sur un appareil intelligent.

La documentation des processus et procédures de travail IDM doit inclure, au minimum, les éléments suivants:

- a) affectations de rôles;
- b) procédures de définition et d'évaluation de la formation et des compétences;
- c) matrice du domaine d'application et des responsabilités;
- d) spécifications des processus de travail;
- e) spécifications de procédures;
- f) spécifications de tâches;
- g) procédures de certification des outils;
- h) collecte exigée des résultats et des formats, structure des données;