



BSI Standards Publication

Intelligent device management

Part 2: Requirements and recommendations

National foreword

This British Standard is the UK implementation of EN IEC 63082-2:2024. It is identical to IEC 63082-2:2024.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 13260 1

ICS 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Intelligent device management - Part 2: Requirements and
recommendations
(IEC 63082-2:2024)

Gestion des appareils intelligents - Partie 2: Exigences
normatives et recommandations
(IEC 63082-2:2024)

Management intelligenter Geräte - Teil 2: Anforderungen
und Empfehlungen
(IEC 63082-2:2024)

This European Standard was approved by CENELEC on 2024-09-17. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65E/1079/FDIS, future edition 1 of IEC 63082-2, prepared by SC 65E "Devices and integration in enterprise systems" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 63082-2:2024.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2025-06-17 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2027-09-17 document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 63082-2:2024 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 60793-1-40:2019 NOTE Approved as EN IEC 60793-1-40:2019 (not modified)

IEC 61158-4-2:2023 NOTE Approved as EN IEC 61158-4-2:2023 (not modified)

IEC 61511 (series) NOTE Approved as EN 61511 (series)

IEC 61511-1 NOTE Approved as EN 61511-1

IEC 61918 NOTE Approved as EN IEC 61918

ISO/IEC Guide 2:2004 NOTE Approved as EN 45020:2006 (not modified)

ISO/IEC 27000 NOTE Approved as EN ISO/IEC 27000

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62381	-	Automation systems in the process industry - Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)	EN IEC 62381	-
IEC 62382	-	Control systems in the process industry - Electrical and instrumentation loop check	EN IEC 62382	-
IEC 62443	series	Security for industrial automation and control systems	EN IEC 62443	series
IEC/TR 63082-1	2020	Intelligent device management - Part 1: Concepts and terminology	-	-

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

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.

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.

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.