IEC TR 63082-1

Edition 1.0 2020-02

TECHNICAL REPORT

colour inside

Intelligent device management – Part 1: Concepts and terminology

IEC TR 63082-1:2020-02(en)

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

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC TR 63082-1

Edition 1.0 2020-02

TECHNICAL REPORT

colour inside

Intelligent device management – Part 1: Concepts and terminology

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40

ISBN 978-2-8322-7855-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INTELLIGENT DEVICE MANAGEMENT –

Part 1: Concepts and terminology

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63082-1, which is a Technical Report, has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

Draft TR	Report on voting
65E/653/DTR	65E/677/RVDTR

Full information on the voting for the approval of this Technical Report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 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 "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The purpose of the IEC 63082 series is to define an environment that enables the effective use of industrial intelligent devices (IID). The documents provide common concepts, terminology, and management activities.

Intelligent device management (IDM) represents activities for managing intelligent devices through the facility lifecycle 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 can be one of many enterprise programs. IDM activities optimize the value from intelligent devices and supports the concepts of integration of data from the production level with business systems. IDM is consistent with smart manufacturing initiatives.

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

While the work processes and implementation practices specified in the IEC 63082 series might be used for non-automation equipment with some diagnostic capability, the IEC 63082 series does not cover these equipment types.

The IEC 63082 series will consist of the following parts:

- IEC TR 63082-1: Concepts and terminology (informative);
- IEC 63082-2: Work process requirements (normative).

IEC 63082-1 describes 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 lifecycle. IEC 63082-1 provides basic knowledge to understand the concepts of intelligent device management necessary to implement an IDM program.

IEC 63082-2 will provide normative requirements for IDM.

INTELLIGENT DEVICE MANAGEMENT –

Part 1: Concepts and terminology

1 Scope

This part of IEC 63082 describes concepts and terminology necessary to understand and communicate effectively about IDM. This document explains the relationship between IDM and other existing asset management standards.

Additionally, this document provides activity structures and concepts associated with IDM programs. This document also introduces the concept of IDM programs for coordination of multiple stakeholders.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

3.1.1
activity
set of actions that consume time and resources and whose performance is necessary to achieve, or contribute to, the realization of one or more objectives

Note 1 to entry: Includes work processes, procedures, and tasks.

[SOURCE: ISO/IEC TR 24766:2009, 3.1, modified – "outcomes" was replaced with "objectives" and the note has been added.]

3.1.2
alarm
notification to the operator of an equipment malfunction, process deviation, or abnormal condition requiring a unique, timely, and documented (predetermined) response from the operator

[SOURCE: IEC 62682:2014, 3.1.7, modified – "an audible and/or visible means of indicating" was replaced with "notification", "timely response" was replaced with "unique, timely, and documented (predetermined) response from the operator".]

3.1.3
alarm management
work processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems

[SOURCE: IEC 62682:2014, 3.1.17, modified — "collection of" was replaced with "work".]

3.1.4
alert
notification to a responsible person of an abnormal condition that can require action with a time tolerance much longer than for alarms

Note 1 to entry: A “responsible person” can include: operators, maintenance personnel, or engineering personnel.

3.1.5
apparatus
device or assembly of devices which can be used as an independent unit for specific functions

EXAMPLE Intelligent measuring and control devices, inspection and testing devices, host systems.

[SOURCE: IEC 60050-151:2001,151-11-22, modified — the example was added.]

3.1.6
asset management
coordinated activities of an organization to ensure the intended capability of assets is available

Note 1 to entry: The capability of an asset is dynamic and asset management will respond to satisfy changing objectives.

[SOURCE: ISO 55000:2014, 3.3.1, modified – "to realize value from assets" was replaced with "to ensure the intended capability of assets is available"; the notes were replaced with a new note to entry.]

3.1.7
calibration
procedure of checking or adjusting (by comparison with a reference standard) the accuracy of a measuring instrument

[SOURCE: ISO 15378:2017, 3.3.2, modified – "process" was replaced with "procedure" and the note was deleted.]

3.1.8
commissioning
procedure prior, or related, to the handing over of a product ready for putting into service, including final acceptance testing, the handing over of all documentation relevant to the use of the product and, if necessary, instructing personnel

[SOURCE: IEC 82079-1:2012, 3.3, modified – "procedures" was replaced with "procedure".]

3.1.9
configuration database
structured collection of parameter settings for intelligent devices

3.1.10
corrective action
action to eliminate the cause of a non-fulfilment of a requirement and to prevent recurrence

[SOURCE: ISO 55000:2014, 3.4.1, modified – "nonconformity" was replaced with "non-fulfilment of a requirement" and the note was deleted.]

3.1.11
covert fault
fault in relation to hardware and software, undetected by the diagnostics, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

Note 1 to entry: These are sometimes called latent faults or unknown faults.

[SOURCE: IEC 61508-4:2010, 3.8.9, modified – "fault" and "and software" were added, "diagnostic tests" was replaced with "diagnostics"; the example was deleted and the Note 1 to entry was added.]

3.1.12
criticality
degree of risk represented by a specified set of levels

3.1.13
device
independent physical entity capable of performing one or more specified functions in a particular context and delimited by its interfaces

[SOURCE: IEC 61499-1:2012, 3.29]

3.1.14
device configuration
procedure that loads parameters into an intelligent device to define its function

3.1.15
device lifecycle
period of time over which a device with a specific model code is developed, brought to the market and eventually removed from the market

3.1.16
device template
set of predefined parameters which characterize a specific device release for a particular type of application

Note 1 to entry: Device templates are normally prepared by the device supplier.

3.1.17
diagnostics
automated function which detects faults, malfunctions, deviations, and/or variations of hardware or software

Note 1 to entry: Diagnostics can be initiated manually for off-line diagnostics.

Note 2 to entry: Diagnostic is used as an adjective and as a generic word.

3.1.18
enterprise
group of organizations sharing a set of goals and objectives to offer products or services or both

[SOURCE: ISO 14258:1998, 2.1.1]

3.1.19
equipment
single apparatus or set of devices or apparatuses, or the set of main devices of an installation, or all devices necessary to perform a specific task

EXAMPLE Intelligent measuring and control devices, inspection and testing devices, and host systems.

[SOURCE: IEC 60050-151:2001, 151-11-25, modified — the note has been deleted and the example added.]

3.1.20
facility
physical entity that is built, constructed, installed or established to perform some particular function or to serve or facilitate some particular end

EXAMPLE Plant, factory, mill, site, or similar production location.

[SOURCE: IEC TR 62066:2002, 3.6, modified — the examples are listed separately.]

3.1.21
facility implementation project
set of activities to put into practice before the facility starts or continues its intended service

3.1.22
failure
<of an item> loss of the ability to perform as required

Note 1 to entry: A failure of an item is an event that results in a fault of that item.

Note 2 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, can be used to categorise failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 3 to entry: Failure could lead to loss of a single function of an item (e.g. secondary function such as diagnostics) not impacting the primary function of the item.

Note 4 to entry: In this definition “an item" refers to "a device".

[SOURCE: IEC 60050-192:2015, 192-03-01, modified – Note 3 to entry was replaced with a new Note 3 and Note 4 to entry was added.]

3.1.23
fault
<of an item> inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the lifecycle, such as specification, design, manufacture or maintenance.

Note 2 to entry: Qualifiers, such as specification, design, manufacture, maintenance or misuse, can be used to indicate the cause of the fault.

Note 3 to entry: In this definition “an item" refers to "a device".

[SOURCE: IEC 60050-192:2015, 192-04-01, modified – Note 3 to entry was replaced with a new Note 3 and Note 4 was deleted.]

3.1.24
host system
functions or tools that digitally communicate with intelligent devices

Note 1 to entry: Includes automated fault handling, management of notifications, and configuration management of intelligent devices.

Note 2 to entry: Functions and tools can be provided on one or more platforms.

3.1.25
incipient fault
imperfection in the state or condition of a device so that a degraded performance or critical failure might eventually be the expected result if corrective action(s) is (are) not taken

[SOURCE: ISO 14224:2016, 3.40, modified – in the term, "failure" was replaced with "fault"; in the definition, "an item" was replaced with "a device", "or critical failure might (or might not)" was replaced with "performance or critical failure might" and "actions are" was replaced with "action(s) is (are)".]

3.1.26
industrial automation control system
IACS
collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

Note 1 to entry: These systems include but are not limited to: a) industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (SIS) functions, whether they are physically separate or integrated.); b) associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems; c) associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Note 2 to entry: The IACS may include components that are not installed at the asset owner's site.

Note 3 to entry: Examples of IACSs include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. IEC 62443-2-4 also defines the proper noun "Solution" to mean the specific instance of the control system product and possibly additional components that are designed into the IACS. The Automation Solution, therefore, differs from the control system since it represents a specific implementation (design and configuration) of the control system hardware and software components for a specific asset owner.

[SOURCE: IEC 62443-2-4:2015, 3.1.8, modified – Note 1 to entry has been added.]

3.1.27
infrastructure
basic physical and organizational structures needed for the operation of an enterprise

3.1.28
inspection
action comprising careful scrutiny of a device and its immediate environment in order to arrive at a reliable conclusion as to the condition of a device

[SOURCE: IEC 60050-426:2008, 416-14-02, modified – "an item" was replaced with "a device" and "carried out either without dismantling, or with the addition of partial dismantling as required, supplemented by means such as measurement," was replaced with "and its immediate environment".]

3.1.29
installation
one apparatus or a set of devices and/or apparatuses associated in a given location to fulfil specified purposes, including all means for their satisfactory operation

[SOURCE: IEC 60050-151:2001, 151-11-26]

3.1.30
intelligent device
industrial intelligent device
IID
configurable device having digital communication with supplemental functions such as diagnostics (3.1.17) in addition to its basic purpose

EXAMPLE 1 Process connected devices, which are in level 1 of the IEC 62264-1 functional hierarchy, such as smart instruments, valves and actuators, analysers, custody transfer meters, electrical breakers, and transformers.

EXAMPLE 2 Control devices, which are in level 2 of the IEC 62264-1 functional hierarchy, such as PLCs, data acquisition subsystems, and dedicated HMI devices.

EXAMPLE 3 Other devices such as RTUs, managed industrial network routers, converters and gateways.

3.1.31
intelligent device management
IDM
formal coordinated business objectives, organizations, work processes, and resources to realize value from intelligent devices

Note 1 to entry: The IDM program is used to achieve setup (provisioning, engineering, configuration and calibration), optimization, diagnostics, maintenance and disposal of intelligent devices over the facility lifecycle based on asset management.

Note 2 to entry: IDM can be applied to multiple facilities of an enterprise or a facility of an enterprise.

3.1.32
intelligent device management program
IDM program
set of coordinated policies, strategies, activities, resources, and organization to achieve IDM objectives

Note 1 to entry: The IDM program is a type of enterprise program.

3.1.33
lifecycle
finite set of generic phases and steps which a system will go through over its entire life history

[SOURCE: ISO 15704:2000, 3.11, modified – “may" was replaced with "will".]

3.1.34
maintenance
activity including supervisory actions, intended to retain an item in, or restore it to, a state in which it can perform a required function

[SOURCE: ISO 14224:2016: 3.49, modified – "combination of all technical and management actions" was replaced with "activity including supervisory actions" and "as required" with "a required function"; the note was deleted.]

3.1.35
management of change
process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control

[SOURCE: IEC 62443-2-1:2010, 3.1.8, modified – "change management" was replaced with "management of change".]

3.1.36
management program
activity that manages a group of related projects and/or work processes in a way that provides benefits and control not available by managing each activity individually and independently

3.1.37
normal operation
operation of apparatus conforming electrically and mechanically within a design specification and used within the limits specified by the apparatus manufacturer

[SOURCE: IEC 60050-426:2008, 426-04-10, modified – "with its" was replaced with "within a" and "apparatus" was added.]

3.1.38
notification
means of communicating a value, state, condition, or symptom to an intended recipient

3.1.39
off-line diagnostics
diagnostics which is performed while the device is out-of-service

3.1.40
operator
person who monitors and makes changes to the production process of the facility

[SOURCE: IEC 62682:2014, 3.1.63, modified — "process" was replaced with "production process of the facility".]

3.1.41
overt fault
fault in relation to hardware and software, detected by the diagnostics, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

[SOURCE: IEC 61508-4:2010, 3.8.8, modified – "fault" and "and software" were added, "diagnostic tests" was replaced with "diagnostics"; the example and note were deleted.]

3.1.42
preventive maintenance
maintenance carried out at predetermined intervals or according to specified criteria and intended to reduce the probability of failure or the degradation of the functioning of an item

3.1.43
proactive maintenance
preventive maintenance (3.1.42) which is carried out based on alerts from the devices

3.1.44
procedure
sequence of tasks with a defined beginning and end that is intended to accomplish a specific objective

3.1.45
prompt
notification that requires the responsible person to take an action that is part of normal operation

3.1.46
resources
people, procedures, software, information, equipment, consumables, infrastructure, capital and operating funds, and time

[SOURCE: ISO/IEC 38500:2015, 2.21]

3.1.47
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014, 3.9, modified — the note was deleted.]

3.1.48
risk analysis
systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO/IEC Guide 51:2014, 3.10]

3.1.49
risk assessment
overall process comprising a risk analysis and a risk evaluation

[SOURCE: ISO/IEC Guide 51:2014, 3.11]

3.1.50
risk evaluation
procedure based on the risk analysis to determine whether tolerable risk has been exceeded

[SOURCE: ISO/IEC Guide 51:2014, 3.12]

3.1.51
risk management
process of identifying and applying countermeasures commensurate with the value of the assets protected, based on a risk analysis

[SOURCE: IEC TS 62443-1-1:2009, 3.2.89, modified — "risk assessment" was replaced with "risk analysis".]

3.1.52
status notification
notification that helps provide the responsible person situational awareness, is part of normal operation and does not require operator action

3.1.53
task
single piece of work that needs to be done and does not have interacting elements requiring management

[SOURCE: IEC 62304:2006, 3.31, modified – "and does not have interacting elements requiring management" was added.]

3.1.54
testing
determination of one or more characteristics of an object of conformity assessment, according to a procedure

Note 1 to entry: "Testing" typically applies to materials, products or processes.

[SOURCE: IEC 60050-902:2013, 902-03-02]

3.1.55
toolkit
set of documents and tools that defines and supports: work processes, project management, and typical configuration

Note 1 to entry: Tools can be hardware and/or software.

3.1.56
typical configuration data set
device template (3.1.16) for a particular facility prepared by the personnel performing the host system configuration

3.1.57
turnaround
scheduled activity wherein a facility is taken off-line for maintenance

EXAMPLE Planned shutdown.

3.1.58
user
hardware, software or human entity that is the initiator and/or target of content consumption

[SOURCE: ISO/IEC 14496-13:2004, 3.18]

3.1.59
vendor
one who sells and/or delivers equipment and/or engineering services

[SOURCE: ISO 35101:20173.16]

3.1.60
work process
set of interrelated or interacting procedure(s) which transforms inputs into outputs

[SOURCE: ISO 55000:2014, 3.1.19, modified – in the term, "work" was added, in the definition "activities" was replaced with "procedures".]

3.2 Abbreviated terms

CR	criticality ranking
EDDL	electronic device description language
EPC	engineering procurement construction
FAT	factory acceptance test
HMI	human machine interface
IACS	industrial automation control system
IDM	intelligent device management
IID	industrial intelligent device
KPI	key performance indicator
MOC	management of change
MTBF	mean time between failures
MTTR	mean time to repair
PLC	programmable logic controller
PPE	personal protective equipment
PSSR	pre-start-up safety review

PV	process value
RAM	risk assessment matrix
RTU	remote terminal unit
SAT	site acceptance test
SIS	safety instrumented system
SIT	site integration test
UML	unified modelling language
WDT	watch dog timer

4 Background and motivation of intelligent device management

4.1 General

Success of monitoring and controlling the physical processes in IACS is built on the appropriate selection of technologies for devices for each application. Aside from input from its direct sensors, a non-intelligent device cannot perceive any other process information. Intelligent devices can have diagnostics that can detect faults in the installation or problems with the application. Each fault or problem could compromise the quality and/or reliability of the measurement and control. Intelligent devices are able to communicate by responding to inquiries or by pushing this information over a network to other intelligent devices. Intelligent devices can also respond to inquiries or push condition information to the balance of the industrial automation control system.

As devices evolve to transmit more data digitally, they deliver more benefits to users as well as the potential for simpler deployment, improved operation and reduced costs. The proliferation of intelligent devices has resulted in an increase in the volume and complexity of data, requiring standards for identifying errors, diagnostic codes, and critical configuration parameters. Intelligent device data delivery standards define what each data point looks like in terms of descriptors and terminology. Process industry standards currently in use for accessing device data, descriptors and terminology in predefined format include IEC 61804 (all parts), IEC 62453 (all parts), and IEC 62769 (all parts).

Other communication channels can be used to link the intelligent device directly to applications such as process monitoring, equipment monitoring, environmental monitoring, energy management, asset management, predictive maintenance, and advanced diagnostics. In some instances, the device data can bypass the real-time control system, reducing the load on the control system and simplifying the overall automation and information system architecture.

Many of the same technologies used in enterprise business systems such as Ethernet have been adapted to automation platforms. As a result, many of the same security and safety concerns found in these systems should be addressed before connecting critical process devices to non-process control networks.

Combining these technology advances will result in better integration of intelligent devices into facility automation and associated information systems. This will make it practical for users to realize the advantages that intelligent devices offer: better process control, higher efficiency, lower energy use, reduced downtime, and higher quality products.

4.2 Established business practices

Business practices are developing or adapting to better support the capabilities of intelligent device technology. These include maintenance, cybersecurity, cost reduction, improved safety and quality, emission reduction, etc. Established maintenance procedures have not yet incorporated intelligent device capability. Organizations' reluctance to change established work processes that were optimized for non-intelligent devices results in forgoing the benefits of built-in diagnostics and digital communications capabilities of intelligent devices.

Established maintenance practices for field devices were sufficiently effective given the limitation of the technology available. In general, these maintenance practices were applied in the following contexts:

- run to failure – used to manage failure modes which were sudden, hidden, or deemed of low impact such that their failure would not impact reliable process operations;
- time based inspection and testing – used to manage failure modes which were both gradual and predictable, such as the mechanical integrity of devices;
- demand maintenance – used to manage failure modes that were either sudden or gradual but unpredictable.

Most intelligent devices contain configuration and diagnostics data that can be used to optimize maintenance practices. In many cases, the promise of intelligent devices in the facility remains unrealized. This is not so much a technology issue as a lack of management understanding of the importance of shifting to new work process appropriate for intelligent devices and addressing the shortage of skilled personnel.

4.3 Objectives of IDM

To use intelligent devices effectively, the following objectives should be achieved:

- required functions;
- basic functions;
- supplementary functions;
- communication functions;
- expected performance;
- accuracy;
- stability;
- response time;
- throughput;
- maximum availability;
- lower failure rate (MTBF);
- shorter repair time (MTTR).

IDM objectives should be achieved with:

- acceptable risk;
- lower likelihood for critical consequences resulting in lower cost of operation;
- minimum deployment cost;
- device, engineering, installing procedures;
- minimum maintenance cost;
- device replacement, spare parts, inspection, testing, calibration, repair;
- computing and logic functions providing key variables for maintenance.

To achieve the above objectives, intelligent devices should be:

- correctly selected, installed, and configured;
- continuously monitored;
- periodically tested;
- maintained at the expected performance level.

Additionally:

- personnel involved should be trained appropriately;
- procedures used should be specified and documented;
- work processes should be clearly defined and documented in the context of IDM programs.

4.4 Conditions for achieving IDM

IDM is best supported in a structured environment that is established during the design and before operation of a facility. Facilities without IDM infrastructure can require hardware and software upgrades. Facilities without IDM infrastructure can use a gap analysis to determine the need for hardware and software modification, new work processes and retraining of personnel. Once the IDM infrastructure is in place, old facilities can be made to perform better with lower risk, and new facilities can be designed, constructed, and operated in a more efficient fashion.

With the implementation of intelligent devices, IDM, and diagnostics based maintenance, significant benefits can be realized as described in 4.5, 4.6, and 4.7 below.

4.5 Benefits and justification of IDM

If intelligent devices are used correctly, they can provide a significant improvement compared to traditional non-intelligent devices in functionality, accuracy, reliability, and total cost of ownership. These benefits include:

- more stable and safer operation of the facility;
- potential efficiencies and saving;
- prevention of lost production by reducing unscheduled shutdowns from equipment failures;
- higher quality product;
- prolonged life of equipment, including the device itself and related apparatus;
- reduction of operating cost to maintain the devices;
- reduction of effort and cost to check the functionalities of the devices;
- reduction of maintenance costs;
- reduction of manual inspection and testing (including safety and compliance benefits).

Intelligent device management has a strong economic value proposition. IDM can produce efficiencies and savings in all phases of a facility lifecycle. The largest incentives for implementing IDM are in the operations and maintenance phase. Detecting and resolving problems before they proceed to failure with associated process impact can reduce unplanned shutdowns. Depending on the application, one savings event provided by the capability of intelligent devices can pay for an entire IDM program investment. Effective use of intelligent devices results in higher accuracy measurements that lead to greater utilization of a facility's capacity. In addition, when device status is incorporated into control algorithms improved process control which results in higher process throughput with reduced variability also leads to better quality products.

The potential to cut maintenance costs is also significant. Many maintenance activities like periodic testing or checking of devices result in "no problem found." These activities traditionally force personnel to enter hazardous areas, climb to areas with poor access, and spend time on unnecessary tests. Device diagnostics as well as the surrounding environment can confirm proper operation without increasing the expense while reducing risk, thus leading to a quicker resolution of operational issues. IDM can significantly reduce manual inspection and testing by using diagnostics – therefore IDM can leave personnel free to optimize existing processes to improve safety and efficiency of the process.

If IDM is implemented appropriately, technicians do not have to go to the place where the intelligent device is installed to get relevant information. Instead, information is provided directly to software tools that organize and present the information to the appropriate personnel in an actionable form. Remote software tools enable maintenance from any location when required.

In addition, because each time a change is made to any piece of equipment it adds stress to the components, by taking corrective action only when required, the device itself will have a longer lifespan.

The new IDM based work processes also provide opportunities to improve:

- data management, the integrity of the resulting signals, the device configuration and settings, and all stages of the signal processing, in addition to accessing the information related to only the process;
- workers' knowledge and knowledge management, which will enable development of best practices and optimization of work processes, through capturing all changes to the individual devices and the resulting analysis;
- maintenance work processes through better understanding of the root causes of device deterioration to focus activities on the source of the reduction in signal integrity;
- the implementation of diagnostic messaging, routine scheduled testing, and inspection procedures.

NOTE Tools and work processes that use the device's built-in diagnostics can improve testing and inspection thus reducing risks to the facility.

4.6 Challenges for implementing IDM

The primary challenge of IDM is its perceived complexity. Unfortunately, the majority of intelligent devices are only used to perform their primary function of providing the process variable. Digital communication and auxiliary functions can maximize the value of the device.

The lack of standardized work processes and available skills at a site are a challenge for dealing effectively with the potential complexity of IDM.

To meet the challenges and capture the benefits of IDM, all stakeholders, such as engineering firms, enterprises, and service providers need to understand their role in proper implementation and use of the tools and support systems for intelligent devices through this set of documents and related standards.

When local support is not available, intelligent devices present an opportunity to provide remote support. Digital networks with appropriate cybersecurity make it possible to access the information needed to troubleshoot a problem remotely without the cost and time of bringing the expertise to the facility.

Intelligent devices can have their functionality altered electronically either locally or remotely. Therefore, the analysis and classification processes in IEC 62443 (all parts) apply to all intelligent devices.

NOTE Rules appropriate for applicable security levels are found in IEC 62443-3-3.

4.7 Relationship of IDM to asset management

IDM is based on asset management concepts that are outlined in ISO 55000 and specified by ISO 55001. Therefore, IDM aligns with the basic requirements specified by ISO 55001.

As mentioned in ISO 55000, the nature and purpose of an organization and its operating environment all have a strong influence on the type of assets that the organization needs to achieve its objectives. An organization's and its stakeholders' intents are translated into design criteria for asset management.

Figure 1 shows the relationship between intelligent device management and intelligent devices in the context of asset management. (An overview and conventions of UML class diagrams are described in Annex A.) Figure 1 through to Figure 8, except Figure 2 are duplicated as an equivalent UML class diagram in Annex B.

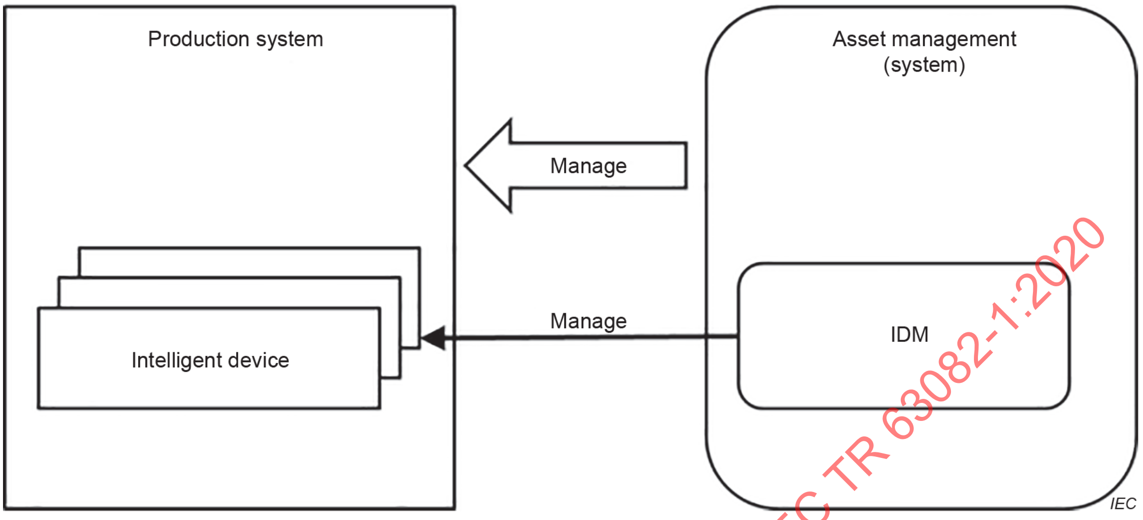


Figure 1 – IDM and intelligent device in the context of asset management

The asset management of the enterprise manages its assets. An intelligent device is one form of asset that is managed by IDM following the principles of asset management, as illustrated in Figure 1.

5 Structure of IDM

5.1 Overview

The objective of IDM is to achieve required functions, expected performance, and availability of intelligent devices with acceptable risk at minimum cost by utilizing features of intelligent devices.

IDM consists of several interactive and interdependent activities. To accomplish IDM goals, the management of these activities requires formal structure and the structure needs to be clearly documented.

Clause 5 provides an introduction to the organizational structures and activities necessary for IDM. This document only introduces concepts and terminology.

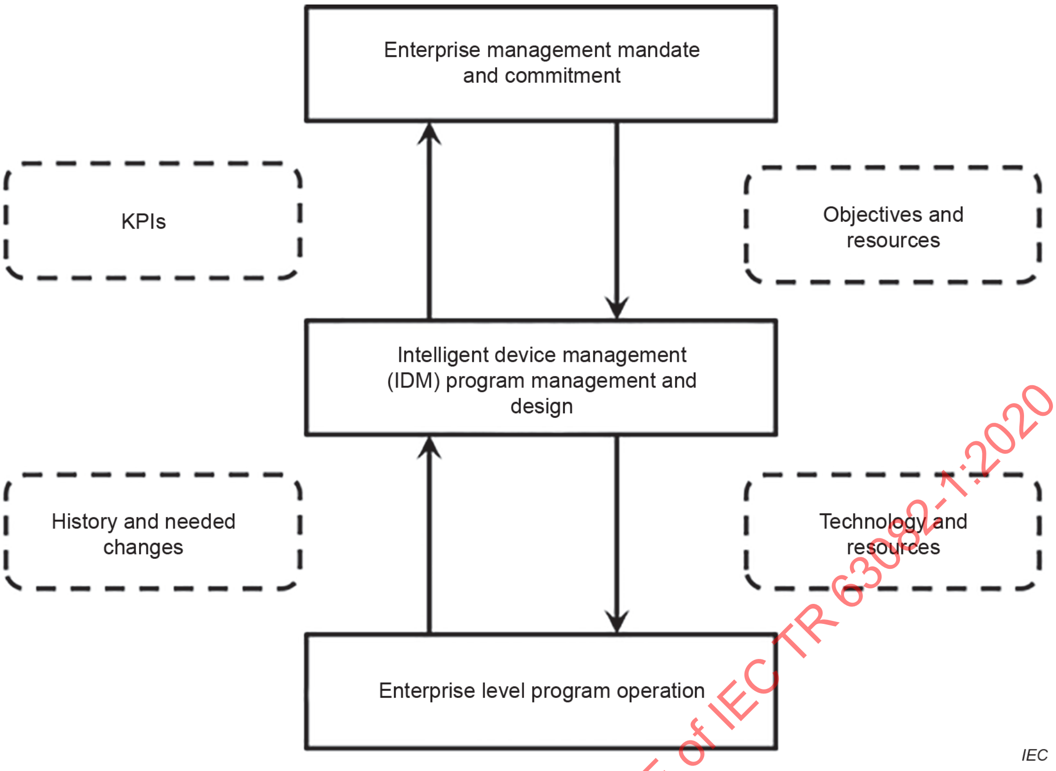
NOTE The details of the work processes and the roles of personnel performing these activities are not covered in this document.

The IDM structure can be implemented for both existing facilities and new facilities.

5.2 Organizational structure

5.2.1 Overview

Subclause 5.2 describes an organizational structure to support IDM activities.


Enterprise management mandate and commitment
KPIs
Objectives and resources
Intelligent device management (IDM) program management and design
History and needed changes
Technology and resources
Enterprise level program operation
IEC

Key

Arrows represent information flow.

Dashed and rounded boxes indicate typical information being transferred.

NOTE IDM coordinates business, engineering, operation and maintenance.

Figure 2 – Positioning of IDM program

Figure 2 shows the positioning of IDM in the context of enterprise business management and IDM work processes. An IDM program translates objectives provided by higher levels of the organization such as business management processes into requirements of technology and resources then passes them to IDM work processes. Similarly, the IDM program translates performance history recorded by work processes into KPIs and passes them to higher or other levels of the organization.

Implementation methods for enterprise business management are non-technical and depend on each enterprise's operating practices. Many enterprise business management stakeholders can impact on the success of IDM. Most enterprise business management processes are created for larger purposes and are not structured to directly manage IDM. A technical and business focus for IDM and a mid-level management structure that can focus on IDM can provide valuable coordination between the IDM work processes and higher-level management.

IDM programs are implemented and supported via IDM work processes. The IDM program requires a well-defined functional structure, but the structure can be tailored to the enterprise's needs.

5.2.2 Structure of IDM activities

IDM programs contain multiple work processes that contain or utilize procedures and tasks. This structure is illustrated in Figure 3 below.

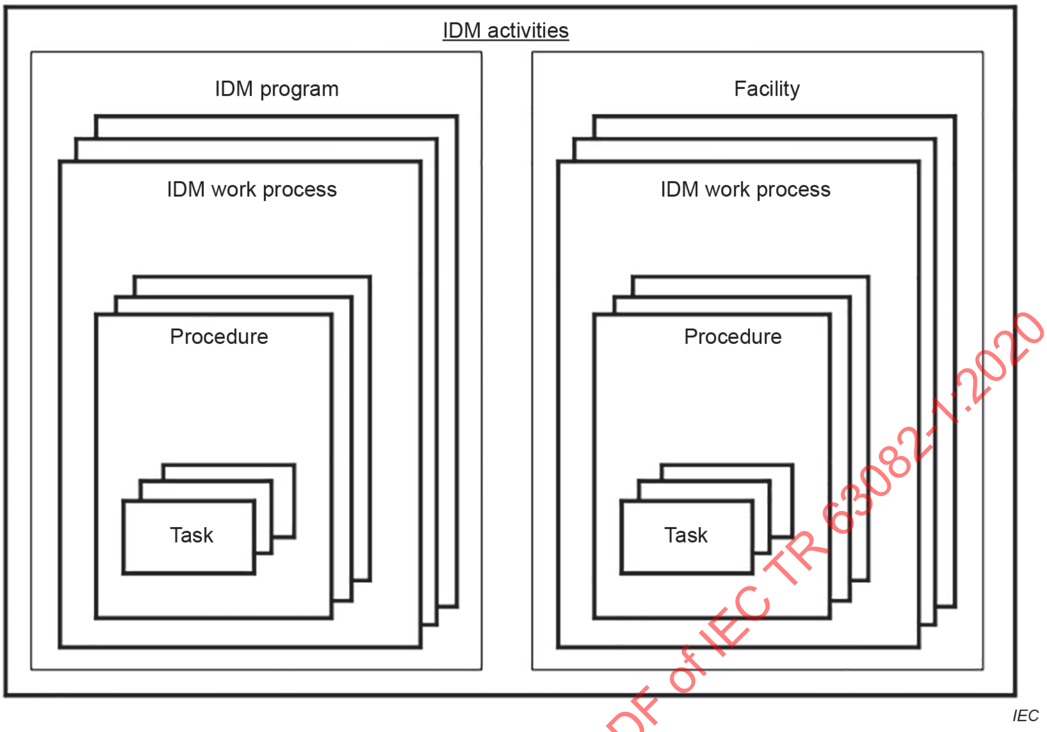


Figure 3 – Structure of IDM activities

5.3 Relationship between IDM program and work processes

IDM contains a large number of activities at several organizational levels and possibly in several internal business units in an enterprise. The activities can be done in house or by contractors. The activities are expected to be performed over several decades of a facility's lifecycle. Documentation explaining how activities fit together and how they are performed should be prepared to coordinate all of these activities by multiple parties over long periods of time.

The following provides a brief outline of an IDM document structure:

- IDM policy;
- IDM risk assessment report;
- IDM objectives including ensuring that intelligent devices are:
  - selected correctly,
  - installed correctly,
  - configured correctly,
  - monitored continuously,
  - tested periodically,
  - maintained at required performance and reliability levels,
  - replaced quickly when they fail,
  - maintained and used by personnel who are trained appropriately,
  - maintained and used with procedures that are properly developed, maintained, and continuously improved,
- IDM program.

Figure 4 depicts an overview of the relationship between the IDM program and work processes. Refer to Annex C which further summarizes IDM objectives and associated work processes.

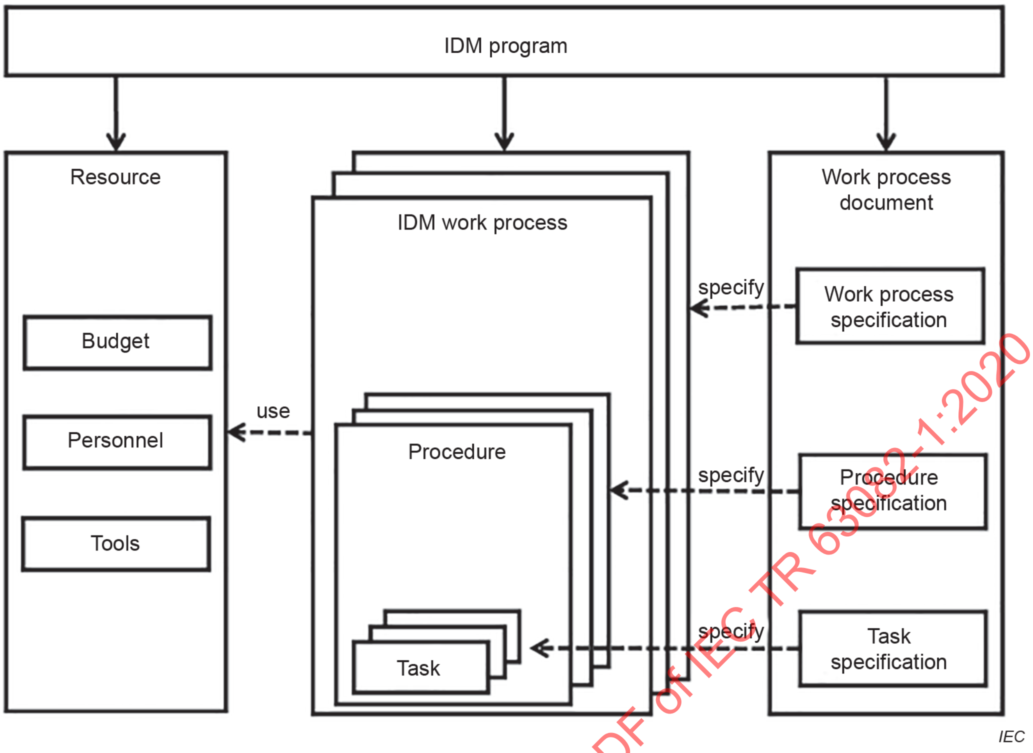


Figure 4 – Structure of IDM program

Since IDM is a part of asset management, the IDM policy is consistent with the asset management policy of the enterprise. The IDM policy is established by the leadership of top management based on the organizational context.

The IDM objectives for each level of the enterprise are developed based on the IDM policy and IDM risk assessment report. The objective of IDM is set appropriately considering the objectives of other management systems. Each IDM objective is translated into the IDM program.

The IDM documents are planned, implemented, and improved by an appropriate document management process.

Table 1 provides an overview of IDM program documents and contents.

Table 1 – IDM documents

IDM document	Description	Contents
IDM policy	Intentions and direction of an enterprise for IDM based on its context as formally expressed by its top management	Scope of IDM Framework for setting IDM objectives Commitment to satisfy IDM requirements Commitment to continual improvement of IDM
IDM risk assessment report	Result of systematic use of available information to identify hazards and to estimate the assessed risk	Potential consequence of failure of the assets Hazards, harms, harmful events Result of device failure analysis

IDM document	Description	Contents
IDM objective	Specific target for an activity of IDM	KPI of IDM and its target Assets covered by the IDM Performance objectives for the assets Strategic plan
IDM program	Set of interrelated or interacting work processes for achieving a particular objective defined by intelligent device management	Resource assignment Work process specifications Procedure specifications Task specifications

5.4 IDM programs

5.4.1 Overview

The IDM program specifies activities to realize the objective. An IDM program is developed for each enterprise based on its IDM policy and IDM objective(s) taking into account its individual organizational context.

IDM programs require:

- balancing multiple and sometimes conflicting goals;
- direct involvement of managers;
- support from technical and maintenance personnel.

An IDM program ensures budget, technical tools, and skills are supplied, and ensures accountability based on quantitative metrics. IDM programs coordinate multiple lifecycles and multiple work processes.

5.4.2 Relational structure of IDM program documents

The IDM program is documented by:

- IDM role assignment;
- work process specifications;
- procedure specifications;
- task specifications.

The IDM role assignment includes organizational roles, responsibilities and authorities specified in ISO 55001:2014, 5.3.

A role that is often utilized for achieving success in an IDM program is a technical, maintenance, and/or business lead that can lead technical efforts and bridge the gap between technical and management functions. This leadership role is a very useful organizational feature for IDM and can be key for successful implementation of this initiative.

A work process specification specifies an IDM work process.

A procedure specification specifies a procedure, which is a part of an IDM work process.

A task specification specifies a task, which is a part of a procedure. A same task can be utilized by different procedures.

NOTE Since specifications of work processes, procedures and tasks are specific to the particular models of equipment, IEC 63082 (all parts) does not intend to specify those particular procedures but it intends to specify generic methodology to specify procedures for intelligent device management.

Figure 5 shows the structure of an IDM program for an enterprise.

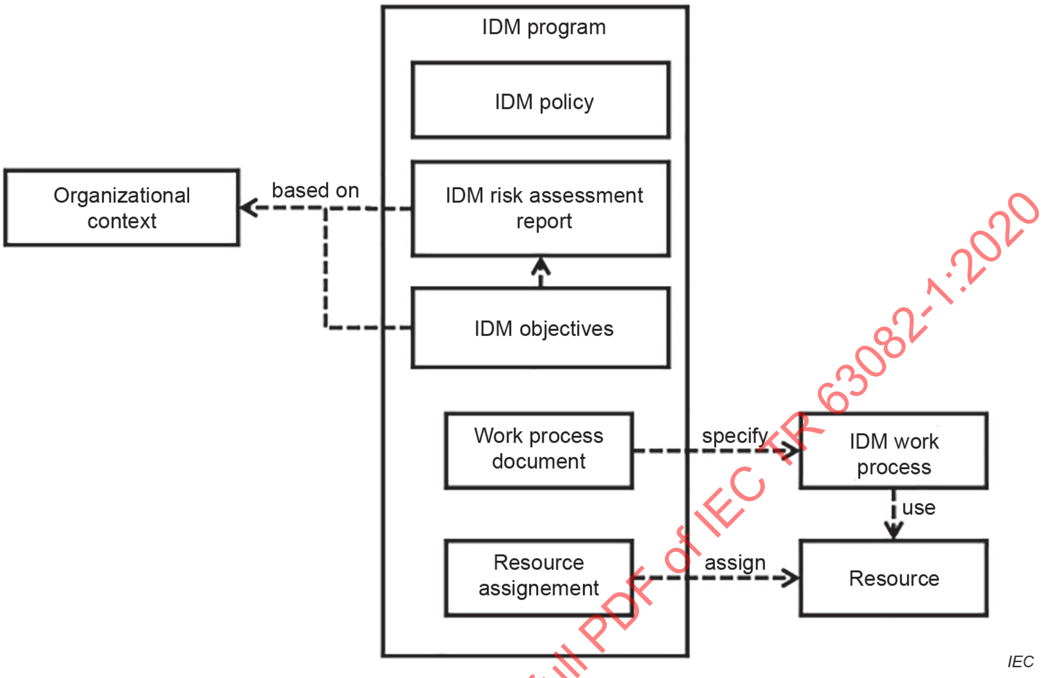


Figure 5 – Structure of IDM program for an enterprise

5.5 IDM work processes

5.5.1 Overview

IDM work processes are technical in nature and are generally directed toward managing or performing a single goal. An IDM work process coordinates procedures of multiple groups of personnel for related activities. An IDM work process is basically expected within a phase of the facility lifecycle.

5.5.2 IDM work processes specification

Every significant IDM work process in every lifecycle phase is specified by an IDM work process specification.

Figure 6 shows the structure of an IDM work process. It includes the following elements:

- work process owner;
- objectives;
- outputs of the work process;
- inputs of the work process;
- start timing;
- procedures;
- interactions among procedures.

The procedure interactions include conditions for initiation of the procedure, but can also include data exchange, synchronization, termination, etc. The condition for initiation includes a procedure to be initiated, procedures that need to be completed before the initiation, and other conditions required for the initiation.

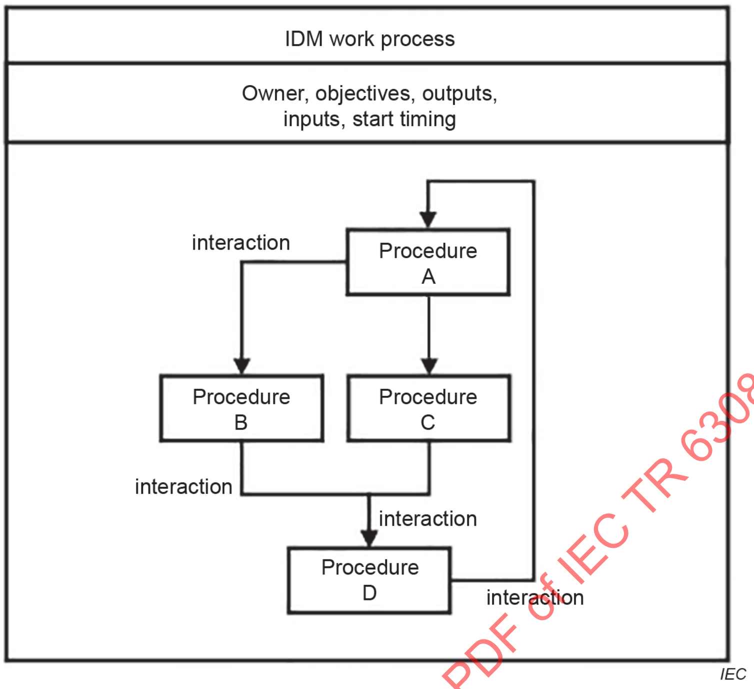


Figure 6 – IDM work process

The IDM work process specification specifies these elements of the IDM work process.

Swimlane charts are the recommended method to represent IDM work processes. The swimlane chart is explained in Annex A.

5.6 Procedures

5.6.1 Overview

Procedures are entirely technical and are comparatively simple, with well defined start and end points. The procedure can coordinate multiple resources, but the interaction is always well defined. Decision points in a procedure are generally well defined and limited by the scope of the procedure.

Procedures often have formal documentation in the form of a list of tasks or a flow chart. Procedures often have explicit instructions of steps necessary to initiate and complete the procedure, as well as requirements to document the results of the procedure.

5.6.2 Procedure specification

A procedure specification defines a procedure, which is a part of an IDM work process.

Figure 7 shows the structure of a procedure. A procedure includes the following elements:

- procedure owner;
- purpose;
- procedure qualification information;
- assigned tasks;
- conditions for starting (e.g. safety approvals);
- conditions for completion (documentation of results).

A task is assigned to a person responsible for its completion.

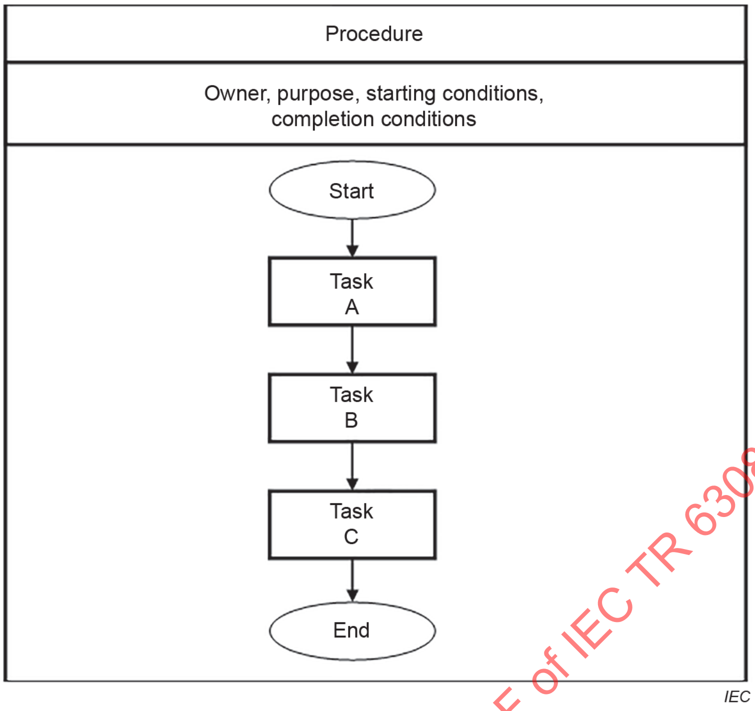


Figure 7 – Procedure

5.7 Tasks

5.7.1 Overview

Tasks are the most simple form of activity that normally needs little interaction or decision. A task is a single piece of work, which is executed by qualified personnel with appropriate assigned resources.

5.7.2 Task specification

A task specification defines a task with its aspects described in 5.7.2.

Figure 8 shows the structure of a task. A task includes the following elements:

- purpose;
- deliverable;
- resource requirement.

The resource requirements include:

- personnel requirement;
- qualified personnel requirement;
- equipment requirement;
- tool requirement;
- information requirement.

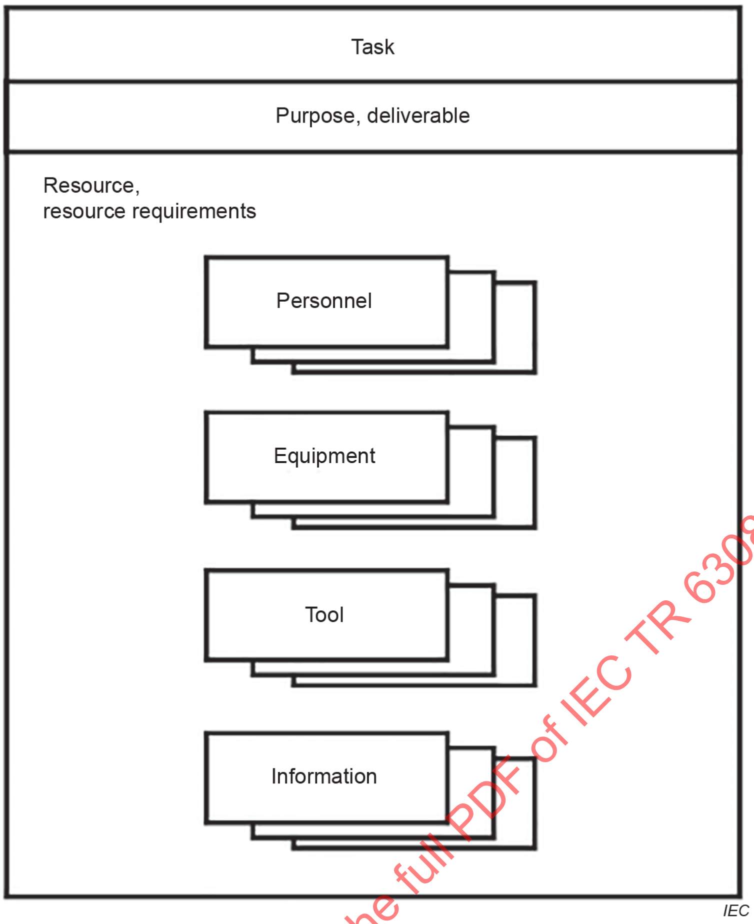


Figure 8 – Task

6 Lifecycles

6.1 Overview

6.1.1 Lifecycle relationships

IDM is an integral part of the multiple lifecycles of an enterprise. Clause 6 describes four lifecycles and the relationship of IDM to these lifecycles. The four lifecycles are overlapping and interdependent. This is typical of enterprise lifecycles that are incorporated into an enterprise program. The four lifecycles are:

- IDM program lifecycle;
- facility lifecycle;
- device lifecycle;
- device technology lifecycle.

The IDM program lifecycle can cover the lifecycles of multiple facilities as shown in Figure 9.

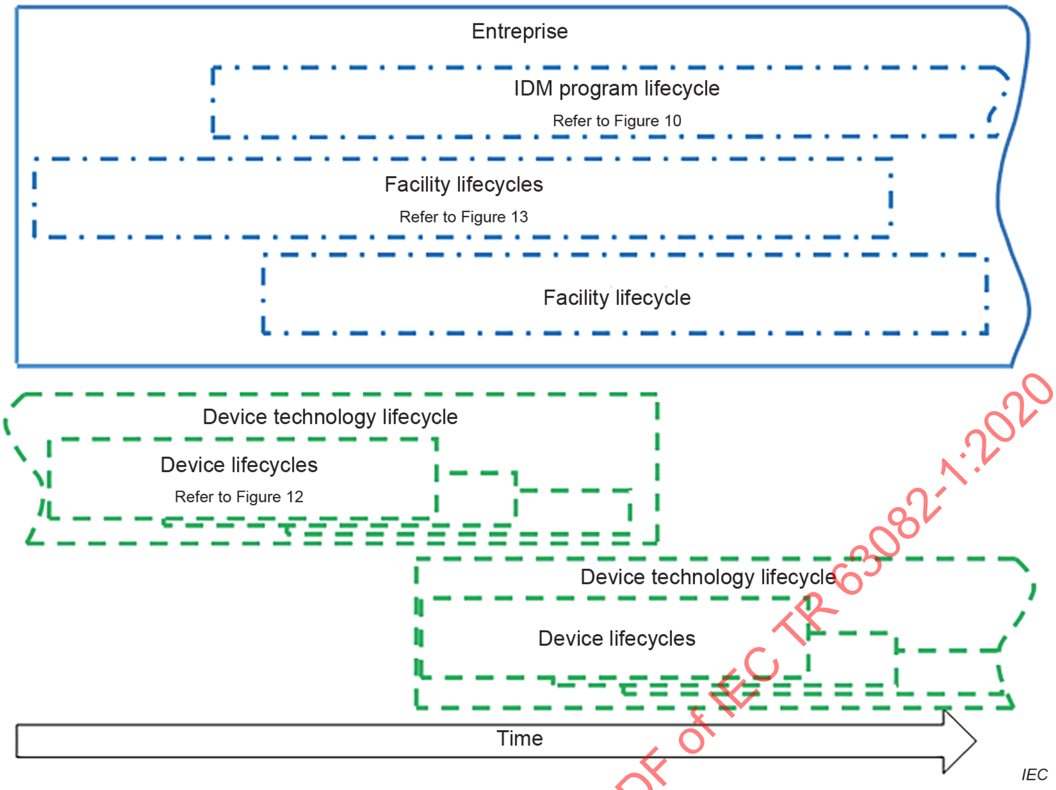


Figure 9 – Timing relationship between lifecycles

6.1.2 Relationship between lifecycles

In practice, the IDM program can be initiated after a facility is already in the operation phase of its lifecycle. Implementation of IDM can be introduced in operating facilities to synchronize existing work processes and establish needed structures. Establishing IDM in an operating facility is challenging and is often beyond the capability of a facility's engineering and maintenance personnel.

While this document illustrates an efficient and mostly linear process for new facilities, most operating companies can modify this to meet the needs of their existing facilities. The end result is very similar, but the implementation can be modified to match the starting point for each facility. For instance, most existing facilities have intelligent devices installed, but they might not have these devices connected to monitoring systems. Small facility implementation projects can rectify gaps in installed monitoring systems so that work processes can be put in place and an IDM program can be established. For these facilities, an audit of installed base capability and deficiency becomes the basis for scope development.

Another structural modification can be done by enterprises that operate a single facility. For these enterprises, the IDM program lifecycle and facility lifecycle can be the same.

Implementation of an IDM program at an operating facility is possible. An IDM program requires investment in infrastructure regardless of whether it is installed in a single facility or across the enterprise. IDM infrastructure can be shared and integrated with other enterprise programs.

6.2 IDM program lifecycle

6.2.1 Overview

Some of the attributes of an IDM program are:

- the scope and boundary limits of an IDM program can change at any time;
- the work process that creates an IDM program and the IDM program itself should never end;
- continuous development is normal for an enterprise program;
- an enterprise program can create or utilize projects, but a project cannot create an IDM program.

An IDM program is one type of enterprise program. An IDM program consists of intangible assets such as ideas, concepts, and intellectual property.

Enterprise programs are management tools. Enterprise programs can allow sufficient management and technical focus to coordinate multiple organizations and activities inside an enterprise and external to the enterprise. The participating organizations can have competing goals in addition to common goals. An enterprise program can provide means to resolve these competing goals and coordinate common goals for maximum effectiveness.

An IDM program provides a convenient name and model for the enterprise and facility level structures that can make IDM work as planned. However, IDM programs can be very different from one enterprise to the next. IDM can be a separate identified management activity in one enterprise, and part of a more diverse program in another enterprise. The structure will work most effectively if it is customized to fit the management style and resource deployment in an enterprise.

6.2.2 IDM program development

6.2.2.1 IDM program phases

Programs can be developed to meet an anticipated need or to address an existing need. IDM programs mostly fall into the existing need category.

IDM activities are in use by an enterprise from the time that the first intelligent device is evaluated for use, until the time that the last intelligent device is removed from service. Removing the last intelligent device from service is not anticipated in the normal course of events.

When intelligent devices are first used, the devices are normally evaluated and supported by highly qualified personnel familiar with new technology. Only a few devices are in use, and ad-hoc work processes and procedures are often used.

When the technology has matured, many different types of devices can be in use in many diverse applications. Critical skills for support can be in short supply, and the aging devices will eventually require updating or replacement with newer technology. The work processes for the initial use of new technology will become inefficient and ineffective for support of mature technology. Formal work processes that can serve an enterprise-wide need can save money, lower risk, and simultaneously improve performance. An IDM program is a natural outcome of efforts to make use of formal work processes to manage intelligent devices.

When developing an IDM program, some up-front work can identify enterprise goals and needs. This will evolve into an operational phase as the IDM program develops. In the operational phase, some implementation work will be necessary at the enterprise level and at the facility level. The exact nature of the starting point, end point, and evolution will depend on the enterprise.

There is no set formula for IDM program development. However, some general principles will identify common steps in the work process. The development steps presented below are logical steps. These steps can overlap in time, and the development is often iterative.

A simplified model for an IDM program lifecycle is shown in Figure 10. This model is accurate for cases where an IDM program is established to meet an anticipated need or when the IDM program is established after a need is revealed through issues with an installed base.

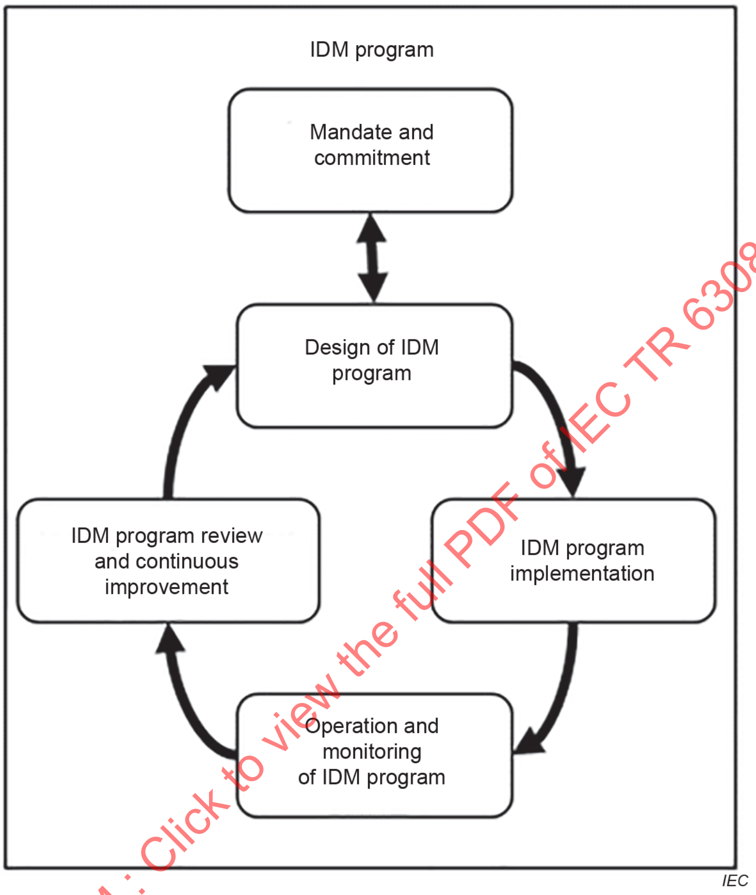

IDM program
Mandate and commitment
Design of IDM program
IDM program review and continuous improvement
IDM program implementation
Operation and monitoring of IDM program
IEC

Figure 10 – IDM program lifecycle phases

Figure 10 shows the continuous improvement "Plan-Do-Check-Act" process that is crucial to IDM program success. Continuous improvement is necessary to manage change inherent to the underlying technology and the long time-span for facility installations.

6.2.2.2 Goals, scope, and objectives

When an enterprise decides to move to formal IDM work processes and procedures, the goals, scope, and objectives should be documented. The goals give guidance on future direction and provide motivation. The scope identifies boundary conditions and can be used to develop external interfaces. The objectives provide measurable targets that can be used to measure success and identify unmet needs. The goals, scope, and objectives will need to be periodically reviewed and updated as conditions change.

6.2.2.3 Gaps, opportunities, and priorities

With a clear mandate, some assessment and gap analysis are necessary. Assessment can include:

- technology installed base;
- tools for managing the technology;
- skill resources;
- other enterprise programs, technical, or management focus areas that impact IDM.

The outcome following assessment and gap analysis is identification of opportunities and a prioritization process to design the IDM program. The prioritization is generally based on opportunities for cost saving and risk reduction.

Enterprises are rarely homogeneous. Some parts of the enterprise can have more extensive gaps than others, and the impact of those gaps can be different across the enterprise.

The gap analysis forms the basis for IDM program development, planning, and implementation. Strategic and tactical decisions are needed before the IDM program can start.

6.2.2.4 Plans, resources, and organization

During the planning step in IDM program formation, some temporary technical and management staffing can be required. This could involve research and development for identified technical gaps or tool development and establishment of external supply relationships to meet the long term needs for technology and personnel.

As plans, technology, and work processes become available, field trials can be useful in testing IDM program operation before more widespread IDM program roll out. The field trial phase can identify areas for further development as well as benefits of formal IDM work processes.

Strategic decisions are needed for IDM program support and tools to serve the needs of facilities. These strategic decisions are not easy to change as they drive long term support optimization and set fixed cost budgets. These decisions also affect enterprise and facility organization structure.

Common support options include:

- support within a facility;
- support within a group of facilities with a common location or business group;
- support at an enterprise level;
- combinations of the above.

The above support options can utilize a combination of:

- in-house permanent staff;
- contracted or temporary assistance;
- support provided by device suppliers.

Decisions about support do not need to be the same for every location or group of facilities in an enterprise. They are often tailored to the type of facility and local conditions. An enterprise program can incorporate a variety of support strategies and still offer all benefits expected of the IDM program.

6.2.2.5 IDM program operation

After the project has been completed and turned over to operations, it enters the longest lifecycle phase associated with ongoing operations. Unfortunately, the technologies associated with IDM do not remain stagnant and therefore continuous monitoring of the effectiveness of the IDM program is critical to success.

Important components of IDM program operations and monitoring include:

- support staff training;
- metrics;
- ongoing communication with all stakeholders (user, vendor, enterprise experts, etc.).

Effective implementation of the above provides the information necessary for the IDM program's continuous improvement.

6.2.2.6 Continuous improvement of IDM

Using the information gathered from KPIs and related metrics obtained from the IDM monitoring program lays the groundwork on which continuous program improvements can be made.

Sharing information between and across facilities as well as the enterprise leads to the development of best practices that can be implemented in the next IDM program renewal cycle.

6.2.2.7 IDM program development results

The result of IDM program development is a clearly documented management mandate and commitment. The mandate and commitment provide the basis for the management and technical focus necessary for efficient and effective management of industrial intelligent devices.

The planning identifies an organizational structure and a functional structure as a basis of IDM program implementation which is compared against the mandate, revised as necessary, then input to improve the IDM program design.

An IDM program functional structure is illustrated in Figure 11.

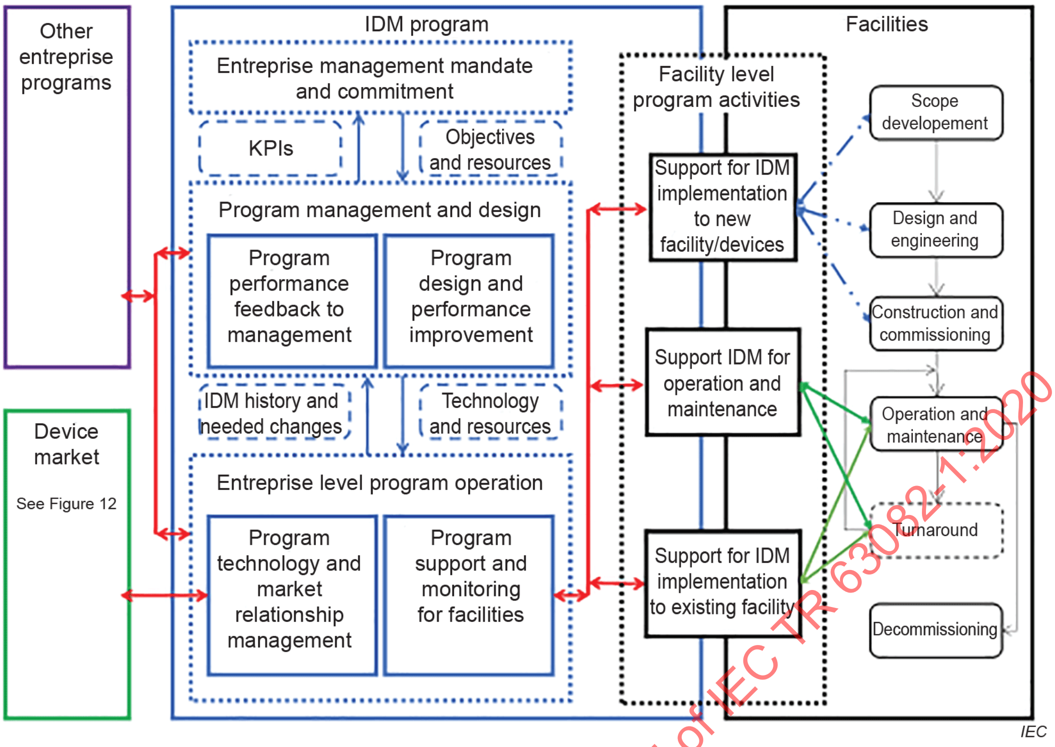

Other entreprise programs
Device market
See Figure 12
IDM program
Entreprise management mandate and commitment
KPIs
Objectives and resources
Program management and design
Program performance feedback to management
Program design and performance improvement
IDM history and needed changes
Technology and resources
Entreprise level program operation
Program technology and market relationship management
Program support and monitoring for facilities
Facility level program activities
Support for IDM implementation to new facility/devices
Support IDM for operation and maintenance
Support for IDM implementation to existing facility
Facilities
Scope developement
Design and engineering
Construction and commissioning
Operation and maintenance
Turnaround
Decommissioning
IEC

Figure 11 – IDM program functional structure

The IDM program functional structure is shown for reference only and represents functions, information exchange, and relationships that are a part of the formal work processes for IDM.

The results of IDM development become a part of the permanent enterprise management mandate and commitment that will be kept current through the IDM program lifecycle. IDM program development does not have to be complete before commencing implementation.

6.2.3 IDM program management and design

6.2.3.1 Resource management

IDM program management and design improvements are activities that support proper utilization of budget and staff resources, and proper introduction of technology changes and support tools. The responsibility and authority needed to make IDM effective and efficient should reside within this function.

6.2.3.2 IDM program design and performance improvement

No organizational structure will fit every enterprise, but IDM will not succeed without sufficient organization and mandate to carry out formal work processes. The IDM program organization will need flexibility to deal with changes in technology and with changes in the enterprise organization.

IDM program organization is necessarily complex because it requires technical and management focus, but it is not independent from other enterprise program level activities. For instance, safety programs and cybersecurity programs impact IDM and can depend on integration with IDM for common support. Coordination of interdependent activities can force resolution of budget and other resource issues by management groups.

6.2.3.3 IDM program performance feedback to management

One primary function of program management is to track performance of the IDM program. Performance metrics measure costs, benefits, and risk management aspects of the IDM program. Analysis of performance measurements are used to make decisions about resource allocation within the enterprise and within the IDM program.

One of the most useful and effective activities within enterprise program management is funding and technical support for common tools, work processes, and technology (toolkits) that can be used enterprise wide. These toolkits can include:

- tools and work processes developed and supported by device vendors;
- tools and work processes developed and supported by system vendors;
- tools and work processes developed and supported within the enterprise.

Toolkit content developed and supported within the enterprise generally supplements or fills gaps in market offerings. Gaps in market offerings generally lead to inefficiency and risk to IDM. Over time, most enterprises have a goal of minimizing market gaps through market and supplier relationship development.

6.2.4 IDM program operation

6.2.4.1 General

Program operation is the part of an IDM program where plans are transformed into actions. This part of any program is dominated by tactical activities rather than strategic activities.

6.2.4.2 Operational activities

Operations are the part of an IDM program where plans are transformed into actions.

6.2.4.3 IDM program technology and market relationship management

Major changes in device technology are disruptive but relatively infrequent. An IDM program should track technology and plan for the timing and rate of new technology adoption. The temporal relationship between device and device technology lifecycles is shown in Figure 9 and Figure 12.

Disruptive technology changes also affect the device supplier market. IDM programs need to have a robust set of suppliers for devices and should have long term relationships with suppliers to maximize device benefits and minimize support cost. Changing device technology or suppliers is disruptive and costly. However, strategic changes are vital to the ongoing health of the organization.

Intelligent devices do not operate as isolated entities. They are assembled into systems with devices from multiple manufacturers. Interoperability is a requirement for these multi-supplier systems. IDM plays a vital role in ensuring long term interoperability.

There are many small changes that are a routine part of the normal device lifecycle. New hardware and software are a routine and normal occurrence for device manufacturers. These small changes can create significant MOC issues for facilities, but an IDM program can make these changes simple and easy to manage.

Device manufacturers face a difficult logistical burden trying to keep facilities informed of changes, and device changes often show up in facilities without the tools and support necessary to make a smooth transition involving minor configuration changes. To address the support problem:

- device manufacturers issue new configuration metadata files for the new device;

- device manufacturers can also issue new configuration templates for new features;
- suppliers or manufacturers can provide automated tools for configuration migration for a new device revision;
- tests can be done to ensure that system integration issues are not generated by the changes;
- an IDM program can deliver a package of support tools to facilities in advance of or as a prerequisite for new or revised device delivery;
- support tools can make pre-packaged and tested engineering migration available for device replacement.

MOC can be simplified by work done for a device that is applicable to all devices of that make and model. Many upgrades do not change a device's base functionality. Generic migration planning, tools, and work processes can eliminate much of the migration engineering required in individual facilities.

6.2.4.4 IDM program support and monitoring for facilities

The primary reason for the existence of an IDM program is for support to facilities. This support extends through the entire facility lifecycle. The existence of an IDM program should significantly ease the burden of dealing with technology issues at any lifecycle phase.

Documentation and training make an IDM program possible. The initial documentation and training will generally be enough to get an IDM program started but will need supplementary material as the IDM program becomes operational. The documentation and training will need continuous maintenance to avoid becoming obsolete. Documentation and training represent a permanent resource allocation for supporting an IDM program.

6.2.4.5 Coordination with other enterprise programs

Some other enterprise programs ensure that functions (i.e. cybersecurity, safety, control, interlock) are designed and performed correctly in systems incorporating intelligent devices. IDM ensures that intelligent devices support these functions. These enterprise programs will only be effective if they work together seamlessly.

Work processes and tools can be shared between different enterprise programs to accomplish common goals. Operational coordination between different enterprise programs will ensure efficiency and effectiveness of support for these common goals.

It is important to understand that an IDM program will be different from an enterprise program that ensures asset integrity for non-intelligent equipment. These enterprise programs are complementary, but not alike. The same can be said for many other types of enterprise programs.

The interaction between complementary enterprise programs will be awkward if not clearly understood. Roles and responsibilities of each enterprise program require careful design, clear documentation, and widespread understanding by all participants.

6.2.5 Facility level IDM program activities

6.2.5.1 IDM program coordination

An important component for IDM program success is the coordination between the enterprise and the implementation(s) at local facilities. The IDM program supports the facility implementation for the complete lifecycle through effective coordination of resources, tools, data, and shared technology.

6.2.5.2 Support for IDM implementation to new facility/devices

IDM can benefit projects by providing assistance such as:

- standard options and selection criteria for scope development;
- work process enhancements;
- supplier selection including qualification and standard agreements;
- templates and toolkits for configuration support;
- information management and handover requirements.

6.2.5.3 Support for IDM for operation and maintenance

IDM can provide direct assistance to operations and maintenance of intelligent devices by providing:

- device revision migration tools, templates, and technical support;
- assistance with root cause analysis or other efforts designed to improve reliability;
- assistance with facility feedback including metrics and audits.

6.2.5.4 Support for IDM implementation to existing facility

IDM can benefit an existing facility by providing:

- template work processes and procedures;
- work process support tools;
- training and competency criteria and assessment.

6.3 Device technology lifecycle

Each successive generation of device technologies (and the IACS they are integrated with) needs different skills and processes for maintenance along with the major differences in design. MOC is needed with each revision of technology. History suggests that this pattern will continue with new generations of device types based on new technologies.

Device technology changes can be disruptive to facilities. Technology changes provide opportunities for new functions and improved performance providing incentive for change. Technology change also causes obsolescence of devices forcing changes that can be inconvenient because of timing and cost. The device technology lifecycles start and end at different times than facility lifecycles and the different timing can be a problem for IDM. For instance:

- a refinery unit was built in the 1940s with float and liquid mercury pressure sensing devices;
- the facility was rebuilt in the early 1960s with force balance pneumatic devices;
- the facility was rebuilt again in the 1980s with analogue electronic devices;
- the facility was rebuilt again in the early 2000s with intelligent devices.

IDM should manage technology selection for new facilities and should determine when updates are needed for existing facilities. In addition, multiple technologies and families of devices are normally used concurrently within a facility. Technology management is an ever changing and complex challenge.

6.4 Device lifecycle

The shortest of the four lifecycles is typically the device lifecycle. Normally, device lifecycles come in releases or model changes that allow migration from one model to the next. However, the entire series of models is typically shorter than the life of a facility.

A device lifecycle consists of phases as listed below and shown in Figure 12:

- device development phase;
- device sales phase;
- after-sales support phase;
- obsolete phase.

NOTE The detail of the lifecycle of a device type model is specified in IEC 62890.

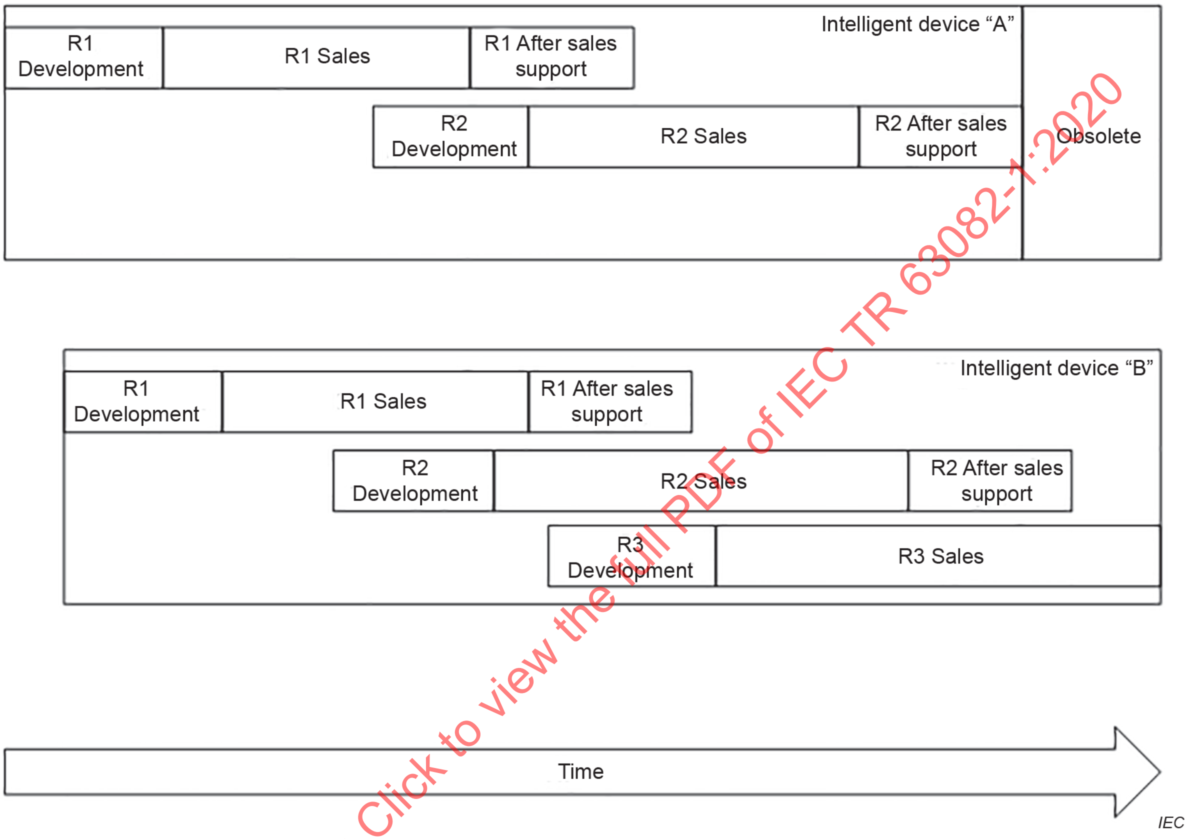


Figure 12 – Timing relationship between IDM device lifecycles

Intelligent devices are built with a wide variety of features and options in addition to their basic function. While the additional features provide value, they also add complexity and preclude interchangeability. These devices generally do conform to some standards and have some level of interoperability, but the added features come with a cost of additional management requirements. Each intelligent device requires the use of software and/or metadata components and therefore revision management is an example of an additional management requirement.

As intelligent devices go through model revisions, new features tend to be added and complexity tends to increase. When intelligent devices are compared between different manufacturers, they support similar functions and features, but their configuration or programming can be incompatible. Enterprises and vendors have significant incentives to manage device diversity and device evolution to make configuration management and maintenance as simple as practical. Some of the benefits of IDM related to device lifecycle are shown in Table 2.

Device changes cannot be synchronized with major revisions of the facility. Suppliers and users of intelligent devices need to cooperate in making these changes manageable. Device revisions can require minor or significant IACS upgrades to accommodate the revision and maintain functionality and performance. For some of the simple changes, the migration can be automated by IACS tools. For more complex upgrades, advanced planning can eliminate the negative effects that can result from unplanned device migration while assuring clearer work processes with simpler MOC in facilities.

Table 2 – Benefits of IDM related to device supply chain management

Role	Without IDM	With IDM
Supplier	Supplier manages each type of device independently.	Supplier works with supplier consortia to provide interoperability registration, easy device replacement, and migration process for devices including, for example, device configuration templates.
Facility	Unlike device replacement, might need engineering support and can occur without prior notification or planning.	Device migration is planned. Device templates, toolkits, and engineering support are supplied from sources external to the facility.
Enterprise	Supplier management is based on only competitive bid for each purchase, for instance a minimum of three bids for comparison purposes is typically required.	Long term supply processes minimize disruption to the supply chain through strategic purchasing agreements. Changes are planned and toolkits are supplied with the change.

6.5 Facility lifecycle

6.5.1 General

Enterprise technical services should be provided for successful implementation of IDM in a facility. An enterprise program is important to the success of implementation of IDM in a facility. Each facility has its own unique lifecycles, it is therefore very inconvenient and inefficient for facilities to try to create their own unique tools for IDM and IDM work processes during individual facility implementation projects.

Facilities are initially built and subsequently modified by a series of projects. Facilities also undergo modification and repair while running to implement some enhancements and issues. Other repairs and modifications are done while the facility is in a shutdown mode as a turnaround.

Starting IDM implementation early in the facility implementation project is also important. A common problem with implementations of IDM (in addition to trying to start from scratch) is to assume that they can delay the start of planning for IDM until construction or commissioning is in progress – or even later. Starting too late will result in a failed implementation that maintenance cannot use, and can create alarm floods for operators and/or maintenance personnel to manage. This late start approach normally results in significant rework of device configuration during or after process start-up, and an ineffective implementation design.

At a minimum, the project will need to install and configure the devices as well as integrate with IDM tools used to work with the devices. Basic infrastructure for IDM is required at every facility and many IDM work processes defined by a facility IDM program can be shared at the enterprise level among multiple facilities. Normal procedure is for facilities to share best practices.

NOTE A facility implementation project will include a number of activities outlined in this document as well other parts of IEC 63082 and related documents.

Facility lifecycle phases and significant activities of each phase are depicted in Figure 13.

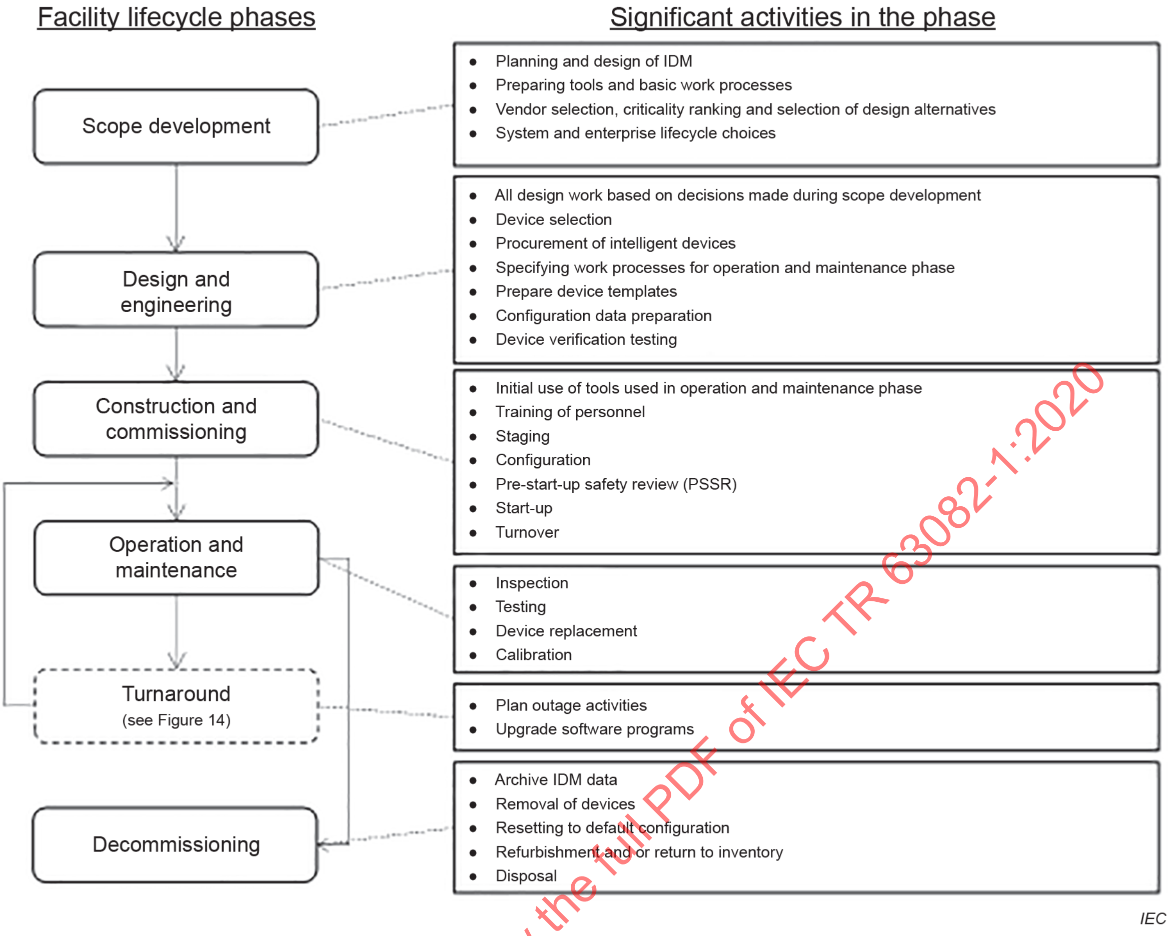

Facility lifecycle phases
Significant activities in the phase
Scope development
Design and engineering
Construction and commissioning
Operation and maintenance
Turnaround (see Figure 14)
Decommissioning
Planning and design of IDM
Preparing tools and basic work processes
Vendor selection, criticality ranking and selection of design alternatives
System and enterprise lifecycle choices
All design work based on decisions made during scope development
Device selection
Procurement of intelligent devices
Specifying work processes for operation and maintenance phase
Prepare device templates
Configuration data preparation
Device verification testing
Initial use of tools used in operation and maintenance phase
Training of personnel
Staging
Configuration
Pre-start-up safety review (PSSR)
Start-up
Turnover
Inspection
Testing
Device replacement
Calibration
Plan outage activities
Upgrade software programs
Archive IDM data
Removal of devices
Resetting to default configuration
Refurbishment and or return to inventory
Disposal
IEC

Figure 13 – Facility lifecycle phases for IDM

The type of project affects activities in various lifecycle phases as outlined below.

Construction of a new facility is often referred to as “greenfield”, where manufacturing is not currently present. This type of project often includes considerable effort to create new infrastructure as part of the scope of work.

Revision of existing facilities, or new construction on existing sites is commonly referred to as “brownfield”. Projects are further divided between revisions that will be done during plant operation and revisions or modifications that require a turnaround. Some projects utilize both revisions during operation and revision during a turnaround. Scope development of plant revision always includes a discovery process to ensure that existing facility documentation is complete and accurate as well as to define required changes. See 6.5.6.

6.5.2 Scope development

6.5.2.1 Overview

Scope development is a collection of development activities, decisions, and documentation of choices. Scope development allows the remainder of a project to proceed to completion with efficiency and integrity. The documentation of choices affecting process integrity made in the scope development provides a basis for change management through the rest of the facility lifecycle.

6.5.2.2 Planning and design of IDM implementation

IDM incorporates many diverse types of work processes by many different groups of people in multiple disciplines. The IDM work processes dedicated to the facility are developed based on the IDM program. IDM programs might not be fully defined prior to the start of scope development. Gaps in IDM programs can be filled by extra work during project definition and execution. Missing parts of the IDM programs can be completed based on the IDM work processes developed during the facility implementation project as part of the continuous improvement phase of IDM program lifecycle as described in 6.2.

6.5.2.3 IDM program lifecycle considerations

A long term support strategy needs to be defined during scope development. A major decision for IDM planning is the amount and type of dedicated resources that are deployed at the facility. Many facilities cannot support full time local resources for every skill or function necessary for long term support of the facility.

Remote monitoring centres have been established for monitoring of assets to assist local resources. IDM can support remote monitoring since diagnostics can be collected and analysed remotely. Use of remote support needs a cooperative local and remote support structure with clear roles and responsibilities for each. This structure also requires significant infrastructure and personnel resources to be able to monitor devices securely from a remote location. Decisions about local and remote support will have an impact on how the IDM system is designed as well as the work processes to support IDM.

6.5.2.4 Selection of design alternatives

Scope development includes selecting design alternatives. Design alternatives include definition of the type and location of a facility, its size and basic functionality, automation requirements, inherent risks associated with the facility, appropriate engineering standards, and appropriate risk reduction measures. These definitions are developed and validated by multi discipline work processes. Enterprise level practices are generally incorporated during scope development. Any new or untried design practices or equipment designs should be clearly identified for the facility lifecycle through to the first turnaround.

The process of selection of design alternatives takes into account the functionality of facilities, the application of intelligent devices in the facility, and the risk assessment results.

Design alternatives also include many decisions that are not part of an enterprise program. The decisions about specific functions and risk reduction methods are often unique to a facility. As the facility specific information is developed, a systematic method for retaining the information should also be employed for success of the project and for long term integrity of the facility. The information needs to be retained in a manner that can survive changes in personnel. It is generally necessary to maintain some level of skills and training (and/or external support) to be able to effectively use the information through the full lifecycle.

Selection of design alternatives affecting IDM that are not correctly made and documented before detailed design begins often have significant negative impact.

6.5.2.5 Preparing tools and basic work processes

Different tools and IDM work processes are needed for each lifecycle phase. These tools and IDM work processes can be working with the same information, but the information will generally be used in a different way in each phase. For instance, data management tools and techniques used during detailed design are generally less useful in the operation and maintenance phase. IDM work processes and tools are needed within phases and also for managing transitions between phases.

Many IDM work processes and tools are not specific to a single project. Toolkits are often maintained and reused by enterprises, vendors, and EPC firms. The reuse of common toolkits improves both efficiency and integrity of the activities where they are employed in any lifecycle phase.

6.5.2.6 Vendor selection

Except in unusual circumstances, vendor selection is normally limited to products that are already for sale. Vendor selection can be part of an enterprise program, as part of a strategic relationship, or it can be a project specific exercise. Selection can be done by an enterprise or by an EPC firm. Supplier selection rules need to be established early in the project scope development in accordance with the IDM program guidelines. Often the selection process is complete before scope development is completed for some major classes of equipment, technology, and/or services.

Vendor selection is executed using the recommended vendor list identified by the IDM program.

Vendors for the facility can be chosen from the following options:

- IDM program pre-determines facility vendor selection;
- facility can choose from the IDM program vendor list;
- facility develops a list independent of the IDM program.

6.5.2.7 Criticality ranking

Criticality ranking described in Annex D is a common industry practice and is necessary for a variety of engineering and maintenance planning activities. Other risk assessment procedures are acceptable if they provide consequence (impact) and criticality (average risk) information. Criticality ranking practices can be applied to risk assessment of intelligent devices.

Criticality ranking information is used in different lifecycle phases as shown in Figure 14. Usage of information from criticality ranking differs depending on the lifecycle phase.

The criticality ranking method works well for individual failures, but does not address the cumulative effect of multiple simultaneous failures.

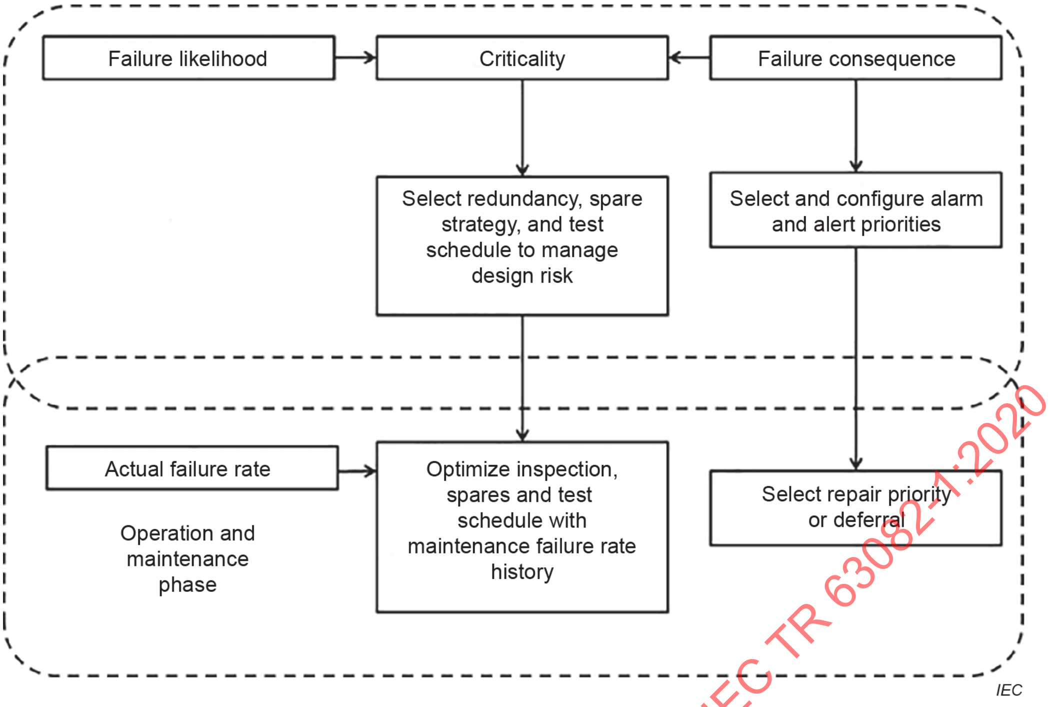

Failure likelihood
Criticality
Failure consequence
Select redundancy, spare strategy, and test schedule to manage design risk
Select and configure alarm and alert priorities
Actual failure rate
Operation and maintenance phase
Optimize inspection, spares and test schedule with maintenance failure rate history
Select repair priority or deferral
IEC

Figure 14 – Criticality usage in a facility

Redundancy design and test schedule development are based on composite criticality in the scope development and design phases, and test schedule optimization. In the operation and maintenance phases, measured instead of assumed likelihood is used to update criticality.

Selecting priorities of alarm and alert in design phase, and planning repair priority and deferral of maintenance use consequence only. Use of diagnostics or redundancy can also be used to reduce the consequence of an individual device failure and thus reduce the need for testing. This is also an area where an engineering analysis during scope development can have a major impact on facility risk with a minimum of cost.

6.5.3 Design and engineering

6.5.3.1 Overview

This phase of the facility lifecycle normally includes all design work based on decisions made during scope development, and as design details are available the procurement processes are completed. Any major conceptual decisions deferments at the start of this phase could possibly delay the implementation of the facility project, and most likely lead to some level of rework.

A number of work process changes as compared to the design of a non-IDM project also need to be considered.

NOTE Details on the work processes below will be covered in other parts of IEC 63082 and related standards.

6.5.3.2 Device selection

Intelligent devices in addition to having the ability to report more than a single process variable, which can impact the number of devices required on a project, can require certain capabilities such as protocol(s) support, support for specific capabilities (e.g. NAMUR NE43 and NE107), or similar functions to be considered as part of the initial selection process. Identifying and agreeing on which capabilities are necessary as early in the design process as feasible will affect which devices are able to support these criteria.

Selection of devices that are still in development exposes the facility to extra risk that requires special management and testing efforts.

6.5.3.3 Procurement of intelligent devices

Procurement of intelligent devices is typically based on preparation of data sheets. Data sheets might need to be modified to provide the ability to specify support for features unique to individual protocols, including the ability to specify which protocol(s) need to be supported. For example, FOUNDATION fieldbus (IEC 61158-1) requires identifying which function blocks are to be included in the device.

The design team can decide how much configuration is done to the devices before they arrive on site.

6.5.3.4 Specifying work processes for operation and maintenance phase

IDM specific work processes for each stage and activity affecting the operation and maintenance phase of the facility lifecycle need to be developed and tested as part of the design process. These IDM work processes are needed when the equipment is being installed.

Implementation of IDM is more difficult and costly if development of support tools and work processes is incomplete during the design phase. Introducing new IDM support tools and procedures into an operating facility is a higher risk activity than doing so as part of the initial design.

If the use of diagnostic coverage is part of the risk reduction process, the associated work processes are also needed to make use of the information and capture the benefits claimed.

6.5.3.5 Preparation of device templates

A number of other considerations related to IDM configuration need to be considered including diagnostics, alerts and other parameters, in addition to those directly related to the process variable, need to be properly configured. Device templates are a proven method to ensure consistency of these settings across families of similar devices.

Device templates should be maintained to reflect changes in each released revision of a device. The design and engineering process should accommodate this change 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.

6.5.3.6 Configuration data preparation

Device templates are an important tool for ensuring consistency of data between the various databases used for each intelligent device. Typical databases for which each parameter should be properly configured and maintained include:

- device configuration file – which parameter settings in an intelligent device and associated databases;
- control system configuration – how the data is received and transmitted to other systems such as the HMI, controllers, and historian is part of the host system configuration;

  NOTE Host system configuration also includes how the system responds to different types of events.
- HMI presentation – how and if activated, which alarms and alerts are presented to the operator or appropriate individual for corrective action;
- asset management tools – what parameters are to be transmitted to systems other than the control system to initiate corrective actions.

The above list is not complete as there are a wide range of other databases such as Historian that are affected by what parameters are and as importantly, are not altered from factory settings during device configuration.

Typicals are similar to but more specific than device templates. Typicals are host system and project specific to address facility specific requirements. The use of typicals is for ‘copy and paste’ in a project configuration.

6.5.3.7 Verification and testing of configuration

Verification of the configuration parameters is conducted during the initial development phase of a project before any devices are available. Additionally, the consistency of configuration data between intelligent devices, host systems and other related equipment is checked. There are many potential opportunities during the construction and commissioning phase to verify the integrity of the many databases as well as the associated device templates and typicals. These integrity tests include but are not limited to those displayed in Table 3.

Table 3 – Verification and testing of configuration

Bench configuration	This is the development and test environment that is not connected to any other systems and often available to test software programs and configurations in the engineering office.
System integration test (SIT)	Testing, typically done offline to verify the integrity of the system in a controlled environment prior to shipment to site with a complete database check but a subset of all the devices connected.
Factory acceptance test (FAT)	Testing typically done in an offline setting where a representative sampling of all devices and nodes used to create the system to be installed is connected and tested for data flow and integrity.
Site acceptance test (SAT)	Testing to verify the integrity of the system after install and prior to turn-over to operations to confirm that all design intents have been met. In many instances the SIT and SAT are done together as part of the loop check procedure.

6.5.4 Construction and commissioning

6.5.4.1 Overview

This phase starts when the design and engineering phase ends and ends with the operational start-up of the facility. As-built revisions of the engineering documents should be finalized before this phase is ended and custody of the facility is permanently transitioned to operations.

6.5.4.2 Staging

Many intelligent devices need some form of environmental protection during the time from receipt of the device at a field site and its permanent install. Devices should be properly identified or tagged. In some cases, part of the device configuration (particularly software tag, device address, or security provisioning) can be done before install.

Some systems and subsystems can be staged, integrated, and tested before field install. However, most field devices are not integrated or configured before the final field install. The work processes for staging, integration, configuration, and testing are varied and complex and will be covered in other documents in the IEC 63082 series.

6.5.4.3 Initial use of tools used in operation and maintenance phase

Preparation of tools, IDM work processes, and training need to be completed in time to use diagnostics during commissioning. A gap in coverage between personnel from the construction and commissioning phases and staff providing long term support needs to be avoided.

Long term support tools can also be used for support of field construction and commissioning activities. Use of these tools during this phase represents an excellent training opportunity for long term support personnel.

6.5.4.4 Training of personnel

Intelligent devices can be complex and use constantly changing technology. It is wise to assume that construction and maintenance personnel are unfamiliar with the devices in general, and that they are also unfamiliar with some of the configuration practices for a particular project. 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 who will be involved in operation and maintenance phases should be started prior to, or during, commissioning in order to familiarize them with the new tools. Adequate training and competency assessment before start-up results in lower risk and greater benefits from IDM during operation and maintenance.

6.5.4.5 Configuration

Configuration is a work process that can take multiple forms. The most basic method is single parameter entry where a technician enters one parameter at a time using an interactive terminal. Single parameter entry is commonly used but because of the inherent inaccuracy of this method it should be supplemented with additional procedures to verify the integrity of the data entered.

A more robust work process than single parameter entry involves download of parameters from a pre-verified database. This method is generally faster and much more accurate than other options.

6.5.4.6 Commissioning

Commissioning typically includes several activities:

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

6.5.4.7 Pre-start-up safety review (PSSR)

Pre-start-up safety review is a final check that handover, training, and general readiness are adequate to start and run the facility safely and successfully. This includes a check of all commissioning assessments.

6.5.4.8 Start-up

This is the final step in the transition from a project to an operating facility. The construction and commissioning phase is generally the final involvement of project personnel, and the initial phase under primary control of operations and maintenance. At the end of start-up a facility should be operating and fully functioning with all training, maintenance tools, work processes, and procedures in place.

6.5.4.9 Handover

The transition processes between the project phase and the operations and maintenance phases can contain many discontinuities.

Because work processes and some of the tools are different from those of the previous phases, the transition to operation phase needs to be carefully managed and planned. The engineering resources that have managed systems prior to handover generally go to new projects and leave the facility to staff who might not be familiar with all of the technical documentation or supporting tools. The transition process from mechanical completion to handover to operations can include many steps including SAT, SIT, simulation testing, process guarantee and others. It therefore needs to be formal and carefully executed.

Facility leadership including management and technical resources are needed during this transition and afterward.

6.5.5 Operation and maintenance

6.5.5.1 Overview

This is the lifecycle phase where the preparation meets the opportunity. Unfortunately, some facilities have waited until this lifecycle phase to start planning. Efficient implementation of IDM is not possible without preparation. Resources are often not available to support implementation in this lifecycle phase.

Continuous evaluation, improvement and management of change of IDM work processes are important in this phase.

Since this is the longest phase in the facility lifecycle, long term support is indispensable. Such support needs to be planned preferably before the facility goes into the operation and maintenance phase.

Troubleshooting skills are not always available in some locations. IDM issues can often be resolved with a combination of local support and remote diagnostics capability.

It is important to note that facility design changes (from complete control system and software upgrades to minor device replacement) can be and often are done during facility operation within the context of a broader facility project.

During this phase, several types of maintenance activity are performed on operating intelligent devices. The following actions are included:

- inspection;
- testing;
- calibration;
- reconfiguration;
- firmware upgrade;
- replacement.

For effective maintenance, the following items regarding the actions should be decided appropriately:

- identifying intelligent devices;
- identifying the type of action to be taken for each device;
- timing of the action to be taken.

In order to identify intelligent devices that require maintenance action; information about status and condition of intelligent devices is collected and analysed. The type of action and timing need to be decided based on maintenance policies which take into account the following factors:

- impact of the current status of the intelligent device on the operation of the facility;
- impact of leaving the intelligent device in the abnormal condition;
- acceptable deferral of action;
- probability and expected time to fatal failure;
- severity of the consequence of the failure;
- cost of the maintenance action.

Types and selection of maintenance process are described in Clause 7. Information obtained from the intelligent device through the network helps the maintenance decision process.

6.5.5.2 Inspection

Some of the inspection items, like the body temperature of a device, can be observed remotely through the network by utilizing digital communication and supplementary functions of the intelligent device. This capability can provide opportunities to reduce the work of inspection in the field and the frequency of visits to a hazardous or inconvenient field site.

Remote condition monitoring can reduce the need for inspection. However, not all inspection items can be remotely observed.

Intelligent devices can support inspection work in the field by providing additional information to the worker through local HMI devices. The local HMI device can be connected to the network or directly to the intelligent device.

6.5.5.3 Testing

Testing is a periodic action to check if functions of the intelligent device are able to work correctly. Some testing items are able to be checked remotely through a network by utilizing the diagnostics capability of intelligent devices.

Even if testing cannot be remotely performed, intelligent devices can support testing in the field by providing additional information to the worker through local HMI devices.

6.5.5.4 Calibration

Intelligent devices can have a supplementary adjusting function instead of a mechanical adjusting screw. Semi-automated calibration procedures can be realized with collaboration between the intelligent device and the reference signal source through the network. This capability can provide opportunities to reduce calibration work in the field.

Additionally, the communication capability of intelligent devices can support semi-automated recording of calibration work. This eliminates manual recording and provides reliable computer readable documentation for calibration, which helps tracking and analysis of the condition of intelligent devices. Calibration can be on an ad hoc or periodic basis.

6.5.5.5 Reconfiguration

Reconfiguration of parameters of intelligent devices is necessary during operation of the facility (e.g. device range change). The capability of remote access to parameters in intelligent devices eliminates the need for a field site visit for the purpose of the reconfiguration.

6.5.5.6 Firmware upgrade

In some cases, upgrading of the firmware version of intelligent devices during the operation phase is necessary. Some types of intelligent devices have the capability of on-line firmware upgrading.

6.5.5.7 Device replacement

Device replacement is necessary because of failure of the IIDs or because of upgrading.

When replacing with the same model and same version of the intelligent device, the replacing device is usually configured with the original configuration parameters in the replaced device. When replacing with a different version or different model device, additional consideration of the configuration parameters is necessary to ensure that the intended functions and performance are retained. Some tuning, testing, calibration and field adjustment specific to the installation can be required in addition to parameter download.

In order to obtain the information for the appropriate configuration parameters, the existing installed configuration data should be consistently preserved and managed. Requirements for the management of configuration data are specified in IEC 63082-2.

6.5.6 Turnaround

6.5.6.1 Overview

Turnaround is a special type of facility implementation project. Turnaround is often used for modifying a facility. Turnaround duration is very significant, because it directly affects the productivity of the facility. Turnaround work can proceed more quickly and efficiently, if work processes, procedures and tasks are well defined and the required resources are assigned to IDM work processes appropriately. Turnaround planning, like all project planning processes, struggles with unanticipated discoveries and changes encountered in the field.

During the turnaround phase, several types of action are performed on installed intelligent devices that are not possible while the facility is running.

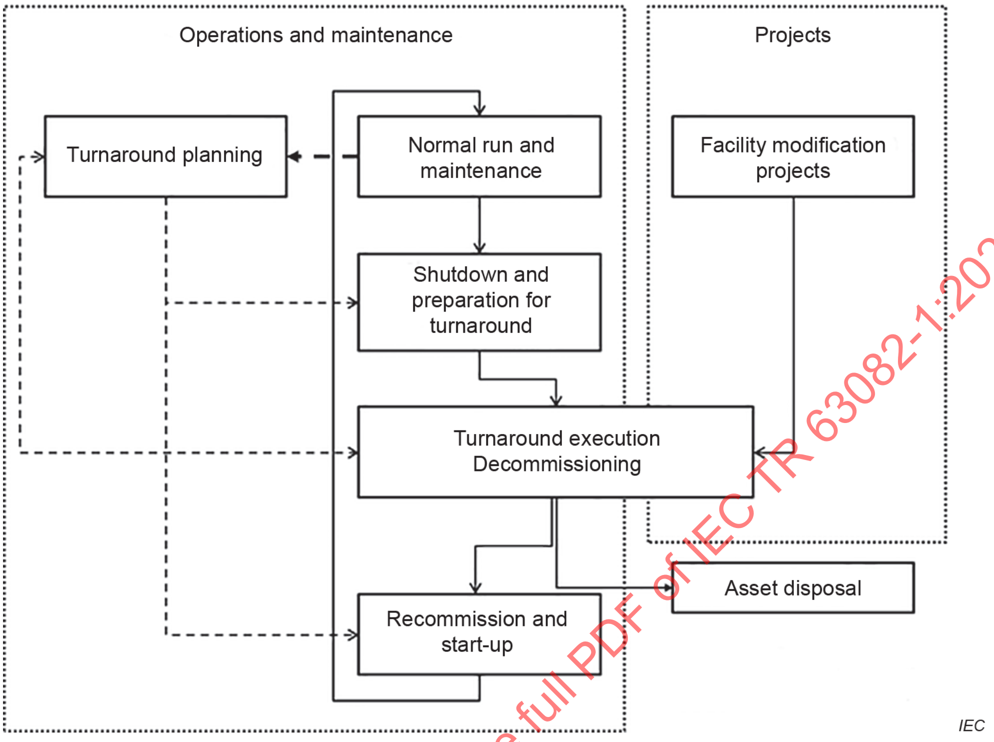
To minimize turnaround time, the number and duration of actions need to be minimized. To develop effective and efficient maintenance plans for turnaround, information collected during the operation phase is used to prepare a turnaround plan for intelligent devices which considers:

- intelligent devices targeted;
- type of action to be taken for each target device;
- timing of the action;
- check of process connections.

IDM helps to collect turnaround planning information in a consistent and efficient way. Tools for IDM are very useful for planning of turnarounds.

Any IDM activity that can be done outside of turnarounds is usually lower cost, less complex, and often lower risk.

As depicted in Figure 15, turnarounds are a combination of project work, which includes facility modification and maintenance activities that are performed during a restricted time window sharing the same work space as the operations, and maintenance activities required for plant reliability.


Operations and maintenance
Projects
Turnaround planning
Normal run and maintenance
Facility modification projects
Shutdown and preparation for turnaround
Turnaround execution Decommissioning
Asset disposal
Recommission and start-up
IEC

Key:

——	Process flow
- - - -	Information flow

Figure 15 – Turnaround process

6.5.6.2 Turnaround planning

The turnaround plan needs to incorporate and consider facility maintenance, modification, or capital projects that can only be completed during the brief plant outage period. Capital projects are described earlier in 6.5. Work items are collected by the turnaround planning time during normal plant operations and maintenance, typically until a “freeze date” early enough before the actual outage to allow for engineering design and equipment procurement to be complete prior to the start of the outage.

Like all project planning processes, turnarounds struggle with unanticipated discoveries and changes encountered in the field during execution. Unfortunately, finding unplanned additional work, such as corroded or worn elements, during turnarounds can be expensive to resolve. However, this discovery work is necessary for completion of a successful production run following the turnaround. Unplanned activities cause a recycle loop back to turnaround planning to incorporate in the current or future turnaround plans.

6.5.6.3 Normal run and maintenance

The facility and processes are operating during this phase. A routine part of the maintenance activities is documenting the condition of equipment and when necessary noting repairs that require a plant outage to execute. These repairs require a turnaround to complete and are therefore submitted to the turnaround planning team for inclusion in the shutdown preparation activities.

6.5.6.4 Shutdown preparation for turnaround

In addition to the planning of the turnaround, significant effort is expended to minimize outage duration through proper planning and preparation to complete as much work as possible in advance of the start of outage so that once the outage starts and the facility is in a safe state, the work itself can begin.

6.5.6.5 Turnaround execution activities

Actions on installed intelligent devices that cannot be accomplished while the facility is in operation are executed during the turnaround phase. These actions are basically the same as those executed during the operation phase except they are executed off-line while the process unit is shutdown.

Some diagnostics can only be performed while the device is out of service. An example of this is the use of valve signature analysis typically done during the initial phase of a turnaround. Diagnostics can also find devices that do not need work during a turnaround at lower cost than traditional inspection and testing methods. The result of effective use of diagnostics is better maintenance integrity at the end of the turnaround.

Functional expansion and revamping usually involves software program upgrading of computer systems that are related to intelligent devices.

In addition, software based products have short lifespans and consequently require regular upgrades. Facility turnarounds offer a lower risk opportunity to perform software upgrades, inspection, testing, and maintenance activities that cannot be accomplished while the facility is in operation.

In some cases, firmware versions of intelligent devices need to be synchronized with the new software program. Part of IDM can include intelligent device firmware upgrades. In this case, preparation of the plan for upgrading of intelligent devices requires identifying which devices need a firmware version upgrade making tracking of each intelligent device revision necessary.

Replacement and/ordecommissioning of equipment is also part of the turnaround execution since it is the only time that the devices are safely isolated.

6.5.6.6 Recommission and start-up

Following completion of the turnaround, the plant is returned to service. This process is known as start-up. During start-up the facility is prepared for the introduction of process fluids following procedures specific to each facility.

6.5.6.7 Asset disposal

During the plant turnaround several assets will have been removed from service or decommissioned and will require disposition as described below.

6.5.7 Decommissioning

6.5.7.1 Overview

Decommissioning refers to the permanent removal of all or a portion of a facility. It can involve disconnection and removal of process fluids, decontamination, as well as disconnection of utilities.

Decommissioning includes removal of intelligent devices from their physical installation in the facility, disconnecting the intelligent devices from the host system and removal of related data from associated databases such as HMIs.

Determination of decommissioning requirements is unique to a facility and is determined at the time of decommissioning, however, there are decommissioning procedures that are standardized including the work processes described below.

6.5.7.2 Archiving IDM information

Regulations can require archiving of data associated with the manufacturing process including IDM information.

6.5.7.3 Removal of devices

IDMs contain a large number of parameters, many of which are stored in a variety of databases. This information is updated and/or cleaned/purged in the appropriate database. These requirements can vary by industry.

6.5.7.4 Resetting to default configuration

Normally each decommissioned intelligent device is reset to the factory setting prior to return to stores. If this practice of resetting is not used, the device needs to be reset as the first part of the configuration procedure.

6.5.7.5 Refurbishment and/or return to inventory

It is likely that an intelligent device removed from service will be salvaged in which case the following actions are required:

- decontaminating, refurbishing, and calibrating intelligent devices;
- verifying part numbers and returning the unit(s) to maintenance stores.

6.5.7.6 Disposal

If part of the facility is not being decommissioned, it is likely the decommissioned device will be refurbished and returned to stores. Alternatively, if the device is not being refurbished, it is likely that it will be disposed of, in which case the device should be returned to the original factory settings to prevent potential release of confidential information.

Though it is not unique to IDM, the enterprise also needs to consider recovery of microprocessors and batteries as mandated by local regulations.

7 Maintenance processes

7.1 Overview

Clause 7 describes work processes that optimize the maintenance of intelligent devices, together with risk management techniques and related technologies. Optimal maintenance management for IDM will be a combination of these work processes.

Maintenance processes provide a way to manage the cost and risk of equipment degradation and failure associated with long term use. There is no single maintenance work process that is optimal for all types of intelligent devices or all applications of intelligent device. A run to failure work process can be the optimum solution for some low risk equipment. Run to failure would be inappropriate, however, for intelligent devices used in process safety applications. This approach could also be a suboptimal solution for long term maintenance cost in installations outside of safety applications. Optimal maintenance management for IDM will be a combination of these strategies. Selecting an effective combination of intelligent device maintenance processes for an enterprise will involve risk assessment of the impact of the device failure.

7.2 Types and relationship of maintenance processes

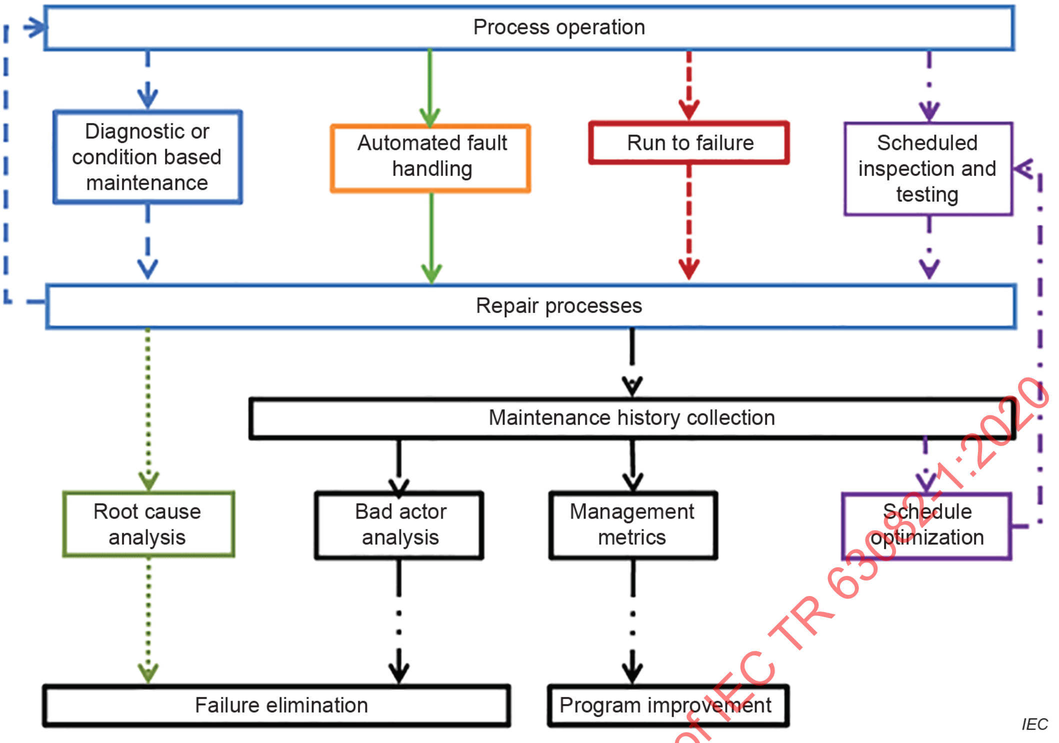
7.2.1 General

Maintenance processes can be loosely organized by relationships and dependencies. Subclause 7.2 will illustrate processes that apply to IDM and describe those dependencies.

Figure 16 illustrates a view of maintenance processes. Each type of process is normally combined with other processes for managing risk for a particular piece of equipment. One process will not fill all needs. Selection and application of appropriate maintenance processes is the key to success for IDM. The method to select the maintenance processes is described in 7.4.2.

There are many types of maintenance processes. A partial list follows:

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



Key:

- - - - Operation and maintenance

——— Automated process

········ Failure process

-·-·- Preventive maintenance

········ Fault analysis

—··— Continuous improvement

Figure 16 – Overview of maintenance process

Choices of maintenance work processes are made at two levels. Some choices are facility (or enterprise) wide and apply to all devices. History collection would be an example. Other choices are specific to applications and affect only devices in those applications or application types. Inspection and testing of critical devices would be an example of this type of choice.

7.2.2 Run to failure

Run to failure maintenance is a valid process for non-critical equipment. This type of maintenance is the result of device degradation processes that proceed to the point where the device can no longer perform its intended function before maintenance or corrective action is initiated. When equipment failure has little consequence on operations, this maintenance process can be employed with little risk. When this process is used for critical equipment, the process leads to loss of production, process consequence, and unplanned repair, also referred to as panic maintenance or crisis maintenance.

Run to failure can occur even with well-developed and executed maintenance processes. The effects of run to failure can be eliminated through the use of redundancy even when diagnostics and fault handling or repair will be too slow to avoid production impact. This type of problem cannot be resolved by work processes.

7.2.3 Diagnostic or condition based maintenance

7.2.3.1 Forms of maintenance

Diagnostics based maintenance is a form of condition based maintenance.

7.2.3.2 Diagnostic opportunity

Diagnostics are generated by a model of some type that predicts expected equipment behaviour, and a check on deviation between actual and expected behaviour. This check can automatically generate notifications (alerts) to allow maintenance planning when equipment performance is somehow abnormal. Diagnostics can be performed continuously on-line, or they can be performed as a part of off-line testing if continuous online monitoring is not possible.

Diagnostics can supplement or replace some portions of manual tests. Diagnostic tests are never perfect and miss some failure conditions. If the diagnostics provide sufficient warning time by notification, maintenance can be performed in time to eliminate the consequence of a failure. When this condition is met, the most efficient of all maintenance processes can be achieved.

Maintenance processes based on utilization of diagnostics can be achieved with intelligent devices and represents a significant opportunity for risk management and cost reduction. Implementation cost for this maintenance process needs little capital investment.

NOTE The opportunity is achieved by use of work processes and procedures that are covered in IEC 63082 (all parts).

7.2.3.3 On-line diagnostics

On-line diagnostics run in intelligent devices fast enough to be within the response time required by the process where the device is applied. On-line diagnostics can be continuous or can be manually or periodically initiated. These diagnostics detect degradation before failure and allow actions to avoid process impact.

Maintenance triggered by automated diagnostics is sometimes called condition based maintenance or proactive maintenance. However, the word proactive means different things to different people and is not a universally understood term. Diagnostics based maintenance is the most efficient and effective form of maintenance in many cases because:

- the repair is done before the device fails;
- maintenance is only performed when it is actually needed;
- unnecessary impact on operations is avoided;
- maintenance can usually be performed in a planned (non-crisis) mode with lower cost and risk;
- failure modes can be configured to minimize impact through automated fault handling.

7.2.3.4 Diagnostic monitoring process

Incipient faults are temporary conditions. They can last anywhere from seconds to weeks, but typically progress to failures before too long. This time period between a diagnostic alert and a failure represents a significant opportunity if a monitoring process that supports troubleshooting and maintenance planning within the time period the incipient fault exists. While the concept of a monitoring and planning process is simple, lack of a monitoring and planning process and the execution of a successful process are not so simple and represent a significant missed opportunity to manage the risk and cost associated with intelligent device application in industry.

7.2.3.5 Off-line diagnostics

Some diagnostics need manual intervention and need the device to be out of service, or even need a shutdown process state for the diagnostic function to be performed. These off-line diagnostics can be automated and can be of significant benefit, but they do not contribute to a maintenance work process (such as automated fault handling) where on-line diagnostics are needed. The primary benefit of off-line diagnostics is in extending test coverage where no on-line diagnostics is possible or available. The off-line diagnostic function is useful to record the normal state of the unused device to find some changes like aging, wear, or degradation.

7.2.3.6 Basic requirements of diagnostics

Diagnostics need proper device configuration. The needed configuration goes beyond the normal configuration of primary function to include configuration of abnormal behaviour. If the benefits of intelligent device management are to be achieved, configuration management of intelligent devices needs more thought and data management than was historically needed for non-intelligent devices. Configuration management is needed for primary functions to be achieved, and the added complexity of diagnostics configuration is well worth the effort. Device templates significantly reduce device configuration management and lower the risk of incorrect device configuration.

7.2.4 Automated fault handling

Automated fault handling will not work without proper configuration of control schemes, logic, or any other consumer of device information.

The most elegant and efficient form of diagnostics based maintenance is achieved when diagnostics are performed continuously in real time and repairs are performed before failure. However, the time for planning is sometimes too short for maintenance. In such cases automated fault handling can be used to prevent process impact. One of the preferred alternatives is to use diagnostic alert conditions to automate fault handling. Diagnostic alerts can be used to set PV status so that control or other applications and operators know that the device is not in good working condition and that alternate actions are necessary. The NAMUR NE107 status signals are one example of automated fault handling configuration.

Alternate actions can be done through redundancy schemes in some cases, but where redundancy is not available, action taken on failure detection can be configured to reduce consequence. This is a significant benefit available from intelligent device management and is generally available with very little cost.

The host system is configured to notify the operator as a result of an intelligent device failure.

7.2.5 Scheduled inspection and testing

Scheduled inspection and testing processes are needed for industrial equipment. These scheduled processes include activities performed during facility operation, and activities that are scheduled during facility outages or turnarounds.

Scheduled maintenance is performed to reduce risk for critical equipment. These processes are designed to reveal or eliminate existing covert faults and identify potential incipient faults. However, the search for these faults usually results in testing and inspection of equipment that is operating normally. Automated diagnostics can reduce the need for (and cost of) manual periodic testing. However, diagnostics do not eliminate the need for manual inspection.

7.3 Other aspects of maintenance

7.3.1 Use of maintenance history

7.3.1.1 General

The collection of maintenance history is critical to being able to analyse the resulting data for trends, improvements, and metrics to determine the effectiveness of the selected maintenance program being implemented.

7.3.1.2 Schedule optimization

The effectiveness and cost of scheduled maintenance can be dramatically improved by collecting failure history in a manner that allows adjusting the frequency of inspection and manual testing based on the frequency of failures. Manual inspection and testing processes normally find infrequent failures, and mostly find no problem with normally operating devices. Thus, scheduled inspection and testing is an inherently inefficient process. The improvements in efficiency with schedule optimization are well worth the effort. Schedule optimization can also show that testing is not frequent enough to manage the risks and that modification of the schedule or design change is needed to achieve the required risk level.

The schedule optimization process and data collection are different for incipient faults and for covert faults. These are often managed by different enterprise programs even though they use similar technology. Both of these are areas of opportunity for IDM.

7.3.1.3 Bad actor analysis

History collection allows identification of “bad actors” or equipment that has abnormally high failure rates. Engineering attention to bad actors can reduce the cost and consequence of failures. This engineering process depends not only on identifying failure rates of particular installations of equipment, but also depends on identification of high failure rates of like equipment used in different applications.

The process of eliminating bad actors needs to identify the root cause of failures so that the cause can be eliminated by design changes. Diagnostics can be of considerable use in identifying root cause as well as automatically registering failure history.

7.3.1.4 Maintenance history collection

Maintenance and failure history is also necessary as a feedback mechanism to understand whether risks are actually being managed at a facility. Without effective history collection (per device), maintenance effectiveness is difficult to evaluate.

7.3.2 Root cause analysis

Root cause analysis is an underutilized technique that allows a rate reduction of all types of failures. The engineering analysis of failures can remove design flaws that cause failures, and can be used to strengthen diagnostics and automatic fault handling so that the consequence of failures is reduced.

Root cause analysis can be applied to high consequence devices or simply to widely used (high volume) devices. Generally, root cause analysis is reserved for high consequence failures for large equipment. However, the large numbers of identical intelligent devices increase the likelihood of identical failures – which can occur in a low consequence application followed by a high consequence application of an identical device. It is quite profitable to analyse intelligent device failures routinely.

7.3.3 Effects of maintenance processes

Maintenance processes are designed to reduce failure rate, failure consequence, or both at the same time. While broad generalizations about the magnitude of these effects are possible, more precise predictions are possible by mathematically modelling the states and transitions in Figure 17.

To effectively and efficiently implement maintenance requires a combination of all maintenance processes.

Types of equipment and the way they are used can have large effects on the consequence of failure. Consequence can vary by many orders of magnitude in risk. Table 4 summarizes one aspect of this risk effect based on size or cost of equipment and the use of redundancy or installed spare equipment.

Table 4 – Failure consequence for non-SIS devices

Equipment type	Non-redundant and non-installed spare	Redundant or installed spare
Large equipment	Very high to high	High to moderate
Small equipment	High to low	Low to insignificant

Some risks, such as from loss of containment, are not mitigated by redundancy, but other failure consequences can be significantly reduced by redundancy. Some large equipment is custom built and might need weeks or months to repair whereas small equipment is more likely to be standardized and much quicker to repair or replace.

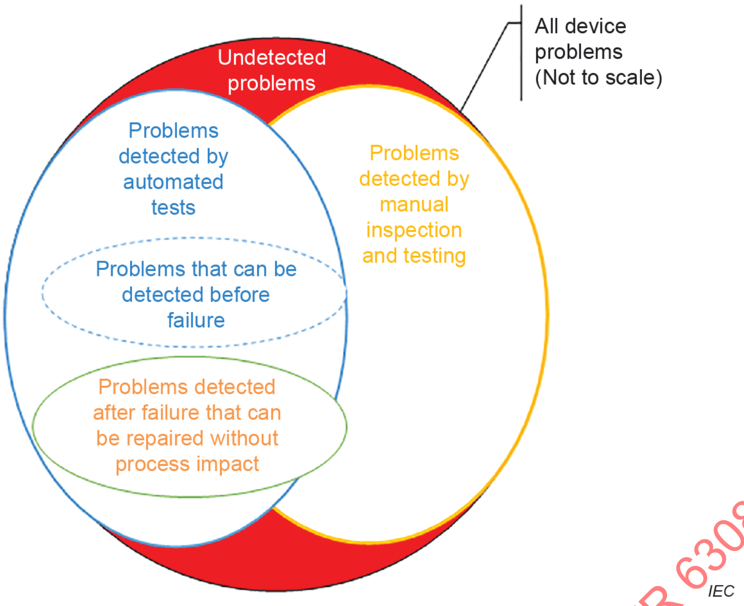
Automation equipment tends to be categorized as small equipment in Table 4. It is common for automation equipment to represent 90 % of the numbered or tagged equipment at a facility in quantity, but only 5 % of the total capital cost of equipment.

As shown in Table 4, redundancy can greatly reduce the criticality of an individual device. However, diagnostics help the redundancy to be fully effective and eliminate covert faults. Once a device in a redundant installation has failed, the redundancy is reduced or lost and the remaining device(s) are now more critical. The loss of a redundant device is reported by diagnostics to initiate repair of the failed device thus maintaining the effectiveness of the redundant installation.

7.4 Relationship of problem detection methods and maintenance strategies

7.4.1 Problem detection optimization

Each maintenance strategy offers an opportunity to diagnose and solve problems. The optimum combination is always a mix of automated diagnostics and manual inspection and testing. This optimum will provide maximum coverage of problems found at a minimum cost for accomplishing the diagnostic tests. This optimum will also provide for minimum impact on process operations if combined with proper troubleshooting and repair procedures.


All device problems (Not to scale)
Undetected problems
Problems detected by automated tests
Problems that can be detected before failure
Problems detected after failure that can be repaired without process impact
Problems detected by manual inspection and testing
IEC

NOTE Key and colours match those of Figure 18 and Figure 19.

Figure 17 – State diagram for IDM

7.4.2 States and transitions

The relationships between processes used for managing intelligent devices need to be clarified. Figure 18 shows states and transitions for the processes. The colour codes and line style in Figure 16, Figure 17, Figure 18, and Figure 19 match for common work processes.

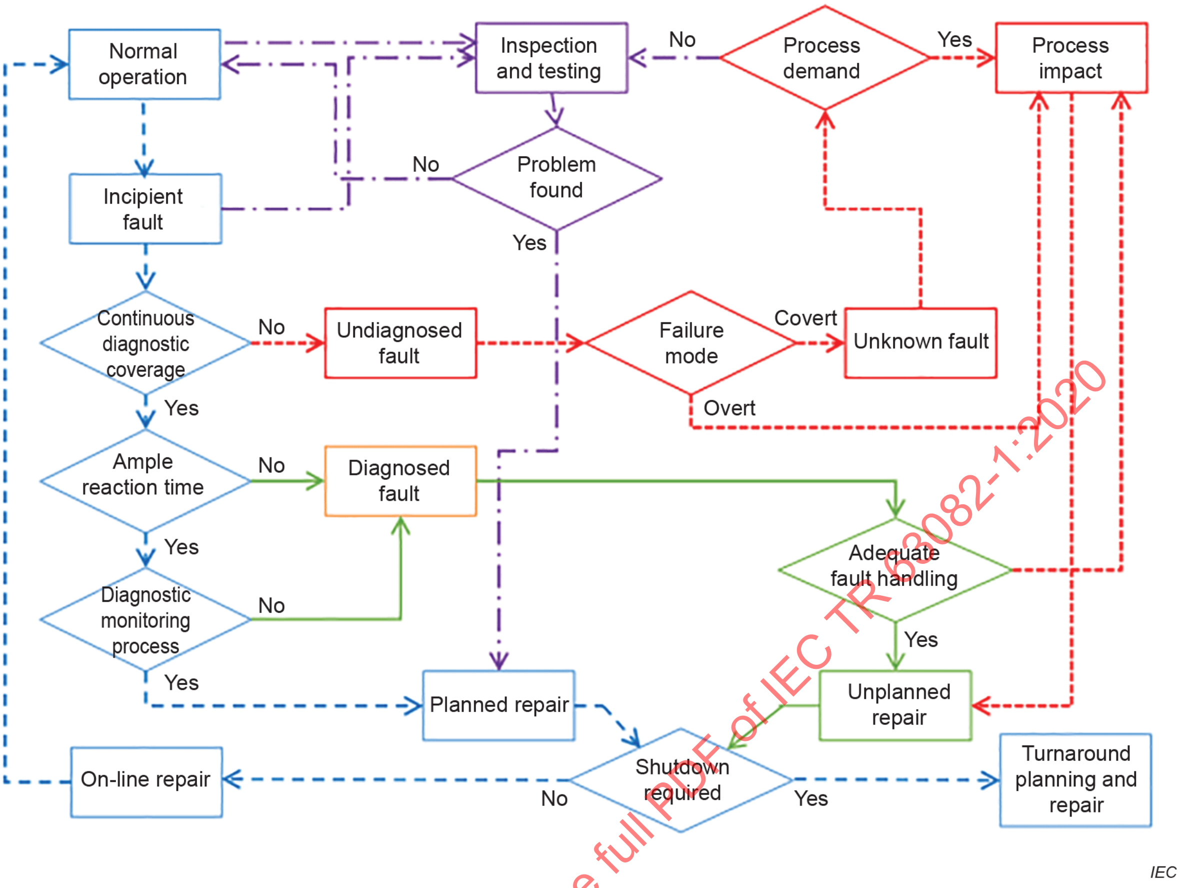


Figure 18 – State diagram for IDM diagnostics based maintenance processes

In Figure 18, diagnostics based maintenance processes can be used to keep operating and maintenance states on the left of the diagram where costs and risks are low. If diagnostics are not present, not configured for use, or are simply ignored, faults propagate to the right side of the drawing where costs and risks are much higher.

7.5 Factors for selection of maintenance process

7.5.1 IDM criticality determination

Criticality determination is necessary to understand which maintenance processes are appropriate for any intelligent devices. Criticality determination and use is covered in 6.5.2.7.

Criticality is needed for design choices, prioritization of maintenance activities and for maintenance management. Criticality ranking is done at a time when engineering processes can proceed – not after the facility is built. Criticality is also effective to improve work processes for facilities already in operation.

Several choices can be made based on criticality. These include:

- the most critical devices applied in health, safety, and environmental protection systems are included in inspection and testing processes;
- the least critical devices can be left in the run to failure category;

  NOTE Once IDM has been implemented, non-critical devices can be included in diagnostic monitoring with minimal incremental investment. For legacy systems, the integration cost for monitoring is difficult to justify for non-critical devices.

- bad actor analysis and corrective action is more profitable for critical devices;

- root cause analysis is often profitable independently of criticality because of the widespread use of identical devices in critical and non-critical applications.

7.5.2 Failure consequences

Consequence is important to determine whether run to failure is a primary maintenance work process for a piece of equipment, or whether run to failure is to be avoided if at all possible. The appropriateness of any maintenance process depends not on the type of equipment, but on the service or application of a piece of equipment and the consequence of failure of that piece of equipment. For SIS, run to failure maintenance strategy might be prohibited by some safety standards.

Consequence also determines what happens after failure. Since the probability of failure is one when the failure occurs, the likelihood (or colour in the risk analysis matrix chart) cannot be used in deferral decisions. Some failures have small consequence for which repair can be deferred until a convenient time, and other failures have a very large consequence and therefore need to be dealt with immediately.

A major factor in maintenance deferral is whether the fault can be repaired on-line (while the process is in operation) or whether the fault needs to be repaired during a process shutdown or turnaround. The cost (and usually risk) for maintenance, that can be performed on-line, is much lower than cost and risk for turnaround maintenance.

Maintenance deferral can be an issue in the case of accumulation of multiple failures where the cumulative consequence is much larger than the sum of individual consequence. The consequence of multiple simultaneous failures can be very non-linear, and predicting the consequence of multiple simultaneous failures is not usually practical. Thus, deferral can lead to larger than expected unmanaged risk.

7.5.3 Types of fault

7.5.3.1 Overview

In order to understand the impact of maintenance processes, it is first necessary to understand basic failure effects. The mathematics relevant to overt and covert faults and associated risks are presented in ANSI/ISA-TR84.00.02.

7.5.3.2 Overt faults

Overt faults are self-revealing faults. These faults have immediate impact at the time of failure. These faults are of primary concern to basic process control systems because they disrupt control when they occur. These faults can also trigger collateral damage when they occur.

7.5.3.3 Covert faults

Covert faults (sometimes called latent faults, hidden faults, or unknown faults) are faults that do not cause any immediate action when they occur. These faults are a primary concern for standby systems such as safety instrumented function in that they disable the safety function without revealing their presence. These faults lower the availability of the standby systems.

Covert faults also present an opportunity for damage upon the occurrence of an overt fault or a process demand. The protection for process impact is lost when covert faults are present.

Covert faults are a target of scheduled inspection and testing processes.

7.5.3.4 Incipient faults

Incipient faults are faults that have not occurred, but degradation processes are in progress that can eventually lead to a fault. Some diagnostics and some manual inspection and testing procedures are designed to detect the progress of incipient faults.

A fault state can occur in a more or less linear process over many years. Other fault states occur by following a nonlinear curve in which failures happen almost instantaneously. Intelligent devices tend to exhibit this nonlinear behaviour.

Manual inspection and testing programs can be effective for incipient faults that progress slowly and linearly, but automated diagnostics are much more effective when degradation to failure is faster and/or non-linear.

8 IDM notification management and utilization

8.1 Notification management

Utilization of diagnostics relies on tools and procedures that support notification management. Many of the basic technologies and processes for alarm management apply directly to management of notifications.

Notification management enables delivery of the correct notification to the correct person with proper context. Standards (see IEC 62682 and ANSI/ISA-18.2) have been written to explain how to manage notifications to operators, but a more general approach is needed for diagnostic notifications including those that need to be sent to other personnel than operators. In fact, most notifications from intelligent devices are directed to engineering or maintenance personnel instead of to operators in order to avoid alarm flooding of diagnostic alerts to the operator.

8.2 Notification from intelligent device

8.2.1 Overview

Notifications include alarms, alerts, prompts, and status notification. Each type of notification has unique characteristics. Table 5 provides a classification of types of notifications.

Table 5 – Notification type

Condition	Operator response required	Other notifications
Abnormal condition	Alarm	Alert
Expected or normal condition	Prompt	Status notification

Notification to operators needs to be carefully chosen from the multiple sources of notifications associated with diagnostics. It is very important to avoid generating nuisance alarms or multiple alarms for non-nuisance diagnostic occurrences.

Individual diagnostic events are difficult to sort through for the basis of engineering and maintenance work processes. There are just too many notifications to use each one separately. Aggregating abnormal conditions into batch style reports makes the troubleshooting process much simpler. The sorting and reporting tools to perform these analyses are readily available in alarm management software packages.

Large numbers of identical devices are used in control systems. One device can be applied in a critical role, and an identical device can be applied in a non-critical role. In this example, the device in the critical role can generate an alarm for a particular diagnostic, and the device in the non-critical role can generate an alert for the same diagnostic. The 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.

Devices that are used in critical and non-critical applications are treated equally in device failure analysis. Since a device type can be used in many applications with different roles, the classification of notifications is more useful for operator actions and repair planning than for engineering analysis.

Device notifications managed by IDM are almost always alerts or status notifications and most of these are delivered to someone other than an operator. Where the notification is used for IDM, the notifications should be delivered to the intended recipient with the correct priority.

8.2.2 Notification type

8.2.2.1 Alarms

Alarm characteristics include the following:

- alarms are always directed to operators;
- alarms have an audible or visual means of getting the operators' attention quickly and indicate the priority of the alarm;
- alarms represent an abnormal condition that needs a specific, timely, and documented (predetermined) response from the operator.

Most diagnostic notifications do not include the above characteristics.

8.2.2.2 Prompts

Prompts are notifications to an operator to take action in response to an expected or normal condition. An example would be a prompt notifying an operator that a sequence in a batch or operating procedure needs manual confirmation or a manually performed action before the batch or procedure can continue.

8.2.2.3 Alerts

Alert characteristics include the following:

- alerts can be provided to operators, maintenance personnel or engineering personnel;
- alerts do not always have predetermined specific responses;
- alerts can have alternative means of notifications than alarms;
- alerts notify the recipient of an abnormal condition that might need action, but usually the time tolerance is much longer than alarms which require operator actions.

Most notifications associated with intelligent devices include the above characteristics. Even though the notifications indicate an abnormal condition, they might only indicate a symptom that needs further analysis before prioritizing and initiating corrective action. Use of alert reports that aggregate and sort multiple alerts can make the process of utilizing alerts much more efficient than trying to deal with individual alerts.

Batch style reports can include a number of alerts from different devices associated with a common cause external to the devices (such as instrument air supply). Batch style reports generally provide a much clearer indication of root cause and urgency than individual device alerts.

The management processes and tools used to manage alarms provide a good basis for the tools and processes used for alerts. However, the different nature of alerts needs some differences in application of the tools and processes. It is useful to make the tools and processes as similar as possible, but it is also important to keep the tools and processes identified and segregated enough so that they do not get confused.

8.2.2.4 Status notifications

Status notifications are sometimes provided as a convenience to indicate that a sequence or procedure is complete. These notifications generally need no action.

8.2.3 Notification sources

8.2.3.1 Overview

Notification sources can be automatic and internal to an intelligent device, automatic but external to a device, or manually generated. No single source of diagnostics can provide 100 % coverage of all types of failure sources, but combining multiple types of diagnostics can provide excellent coverage.

8.2.3.2 Automated internal device diagnostics

Internal diagnostic algorithms are in almost every intelligent device and can provide a high degree (> 90 %) coverage of faults of intelligent devices. These diagnostics typically require configuring some parameters of the intelligent device to be utilized effectively.

8.2.3.3 Automated external device diagnostics

Intelligent device internal device diagnostics cannot detect all faults: as a result, external diagnostics are also used. An example of an external diagnostic is a watchdog timer (WDT) in the host system to detect when communication with an intelligent device is lost. Another example is where several measurements can be compared in a host system to detect when a measurement is incorrect. In some instances, external diagnostics also require additional device configuration by the user.

8.2.3.4 Manual inspection and testing

Manual inspection and testing can include a variety of procedures including inspection of installation integrity (such as corrosion or insulation integrity) or manually performed work such as checking purges or calibration checks. Many manual inspection and testing procedures interfere with measurement integrity and require flagging of process data (PV status).

8.3 Notification delivery mechanism

8.3.1 Overview

Notifications resulting from a diagnostic condition are delivered in multiple forms. All of these forms are useful for a purpose, but they can be confusing if not configured and utilized properly. The confusion can arise if the notification is not directed to the proper person, or if multiple notifications are delivered to the same person from a single source. Notification source, destination, and routing options can best be visualized with a graphic representation as shown in Figure 19.

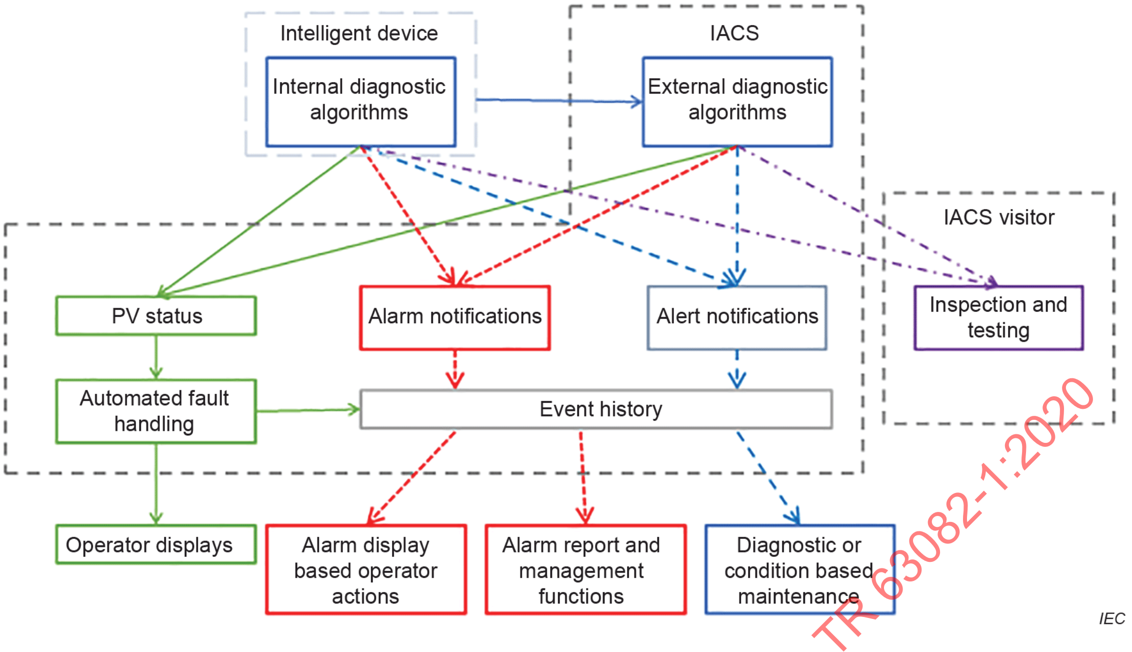

Intelligent device
Internal diagnostic algorithms
IACS
External diagnostic algorithms
IACS visitor
Inspection and testing
PV status
Alarm notifications
Alert notifications
Automated fault handling
Event history
Operator displays
Alarm display based operator actions
Alarm report and management functions
Diagnostic or condition based maintenance
IEC

Figure 19 – Notifications routing for IDM

Notifications for IDM should be directed (by configuration) from the appropriate source to the appropriate destination with appropriate priority. As a result of this requirement, notification configuration is application dependent and cannot be predetermined prior to completing the necessary engineering and design based on device application and criticality. Configuration of the IACS and device is necessary to accomplish the notification routing.

8.3.2 Device alert

Device alerts contain the report of a specific device symptom or problem. In almost all cases they are useful for troubleshooting by engineering or maintenance personnel, and they do not have actionable or unique information that can be utilized as operator alarms. These notifications are most useful if they are aggregated into pre-sorted reports which can form the starting point for diagnostic monitoring and corrective action processes.

8.3.3 Process value (PV) status

Intelligent devices often have the ability to set and deliver status flags along with process value. These status flags are very useful for (and are the basis for) automated fault handling and can be useful for operator actions. At a minimum, operators need to be made aware of PV status in all displays or reports they access.

PV status needs to be delivered in a format defined by NAMUR NE107 if possible. An alternate mechanism for status flagging of 4 mA to 20 mA signals is available with one option described in NAMUR NE43 that can be implemented and useful with legacy systems that do not support digital integration.

PV status aggregates a number of device symptoms into a simple status format. This loss of granularity of information makes these flags less useful for troubleshooting processes than the individual status alerts.

8.3.4 Operation (control) mode

When a PV status indicating a failure state is delivered to a control, interlock, logic software program, or reporting software program, the target software program needs to take some fault handling action if possible. For control algorithms this is often called mode shedding. In some cases, an operator action is needed as a response to the fault handling or mode shedding. If this is the case, the mode shedding event is the most likely source for an operator alarm associated with the diagnostic based event.

8.4 Action responding to notification

8.4.1 Overview

IDM notification management deals with real time activities, semi real time activities, and planned activities. Figure 20 provides a diagram of the relationships between real time (including time critical activities and automated activities), semi real time activities, and planned activities.

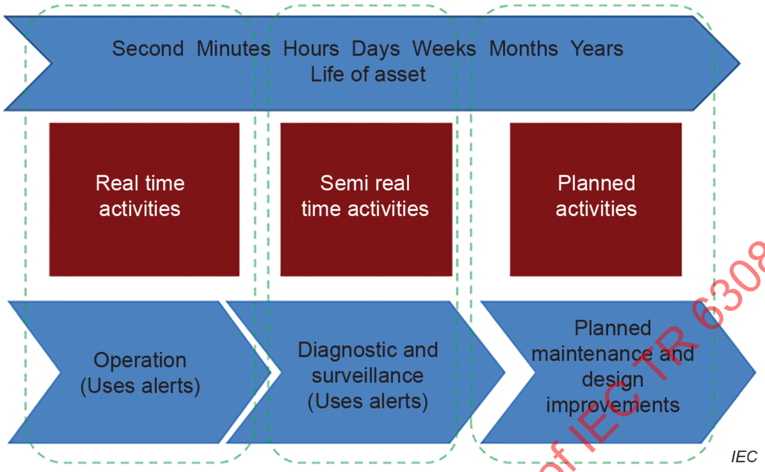

Second Minutes Hours Days Weeks Months Years
Life of asset
Real time activities
Semi real time activities
Planned activities
Operation (Uses alerts)
Diagnostic and surveillance (Uses alerts)
Planned maintenance and design improvements
IEC

Figure 20 – Relationship between real time, semi real time, and planned activities

8.4.2 Real time automated responses

Abnormal conditions that need a response within seconds generally require an automated response. The notification of this automated action to the operator might or might not be an alarm. An example would be control mode shedding due to failure of a measurement device.

For device diagnostics to be effective in preventing mis-operation of controls, the diagnostics are expected to operate faster than the cycle time of the controls so that up to date PV status information is always available. In fact, diagnostics rarely operate this fast. PV updates and control processes generally run somewhat faster than device diagnostics.

Table 6 shows the benefits from real time automated responses.

Table 6 – IDM benefits from real time automated responses

Time scale	Without IDM	With IDM
Seconds	Device diagnostics and control algorithms are not configured for automatic failure handling, failure effects are random.	Device diagnostics are configured and control algorithms provide optimum action on failure, failure consequences are reduced and more predictable.

8.4.3 Real time operator responses

Abnormal conditions that need an operator action within minutes to hours are generally handled through alarms. The intent of alarms is to allow operators to take action quickly enough to mitigate or correct mis-operation by control or process equipment failures. The time available can be 5 min or longer.

Table 7 shows the benefits from real time operator responses.

Table 7 – IDM benefits from real time operator responses

Time scale	Without IDM	With IDM
Minutes/hours	Live data displays, alarms, and trends confuse operators by not displaying correct data quality and by not alerting failure, or by hiding failures in nuisance alarm floods.	Operators are always made aware of status in all data sources and are properly notified when they need to take action. Operator effectiveness is improved.

8.4.4 Semi real time responses

Many device diagnostics need no response (they are advisory) or the response might be needed in days or weeks. The response can be from operations, engineering, or maintenance resources depending on the local staffing process. Notifications for these conditions utilize alerts.

An example of this sort of diagnostic alert might be an incipient fault of a device. This condition exists when some sort of device degradation process is detectable, but the device is still functioning. This is a common occurrence for device alerts and allows for maintenance personnel to respond before failure. The differences between responses before versus after failure include:

- allowable time to plan for repairs;
- occurrence of damage from the failure;
- occurrence of collateral damage from the failure.

The savings from repair or replacement of incipient faults can be orders of magnitude more than the cost of repair of the device.

Table 8 shows the benefits from semi real time responses.

Table 8 – IDM benefits from semi real time responses

Time scale	Without IDM	With IDM
Days/weeks	Maintenance is done in crisis mode on devices that have already failed and might have caused collateral damage.	Maintenance is done on devices that have incipient fault notifications but have not yet failed or affected operations. Maintenance efficiency is improved by removing panic from the process. Business disruption and repair costs are significantly lowered by reduction of failures. Collateral damage can be reduced and/or minimized.

8.4.5 Longer term planned responses

Some conditions need more time for response. Examples of these conditions include those that need a process shutdown for repair and/or an engineering redesign to address a problem. Initial discovery of these conditions can be from diagnostics, as well as from manual inspection and testing procedures.

Table 9 shows the benefits from longer term planned responses.

Table 9 – IDM benefits from longer term planned responses

Time scale	Without IDM	With IDM
All time scales	All troubleshooting is done at the physical installation. A facility needs to have all skills available locally or pay for travel by experts to the facility.	Remote engineering analysis and support is routine. Collaboration with technology experts is supported by remote access tools, formal procedures, and commercial agreements. Location personnel have support when needed. Remote access can speed diagnostic processes while minimizing travel requirements. Corrective action can be accomplished more quickly.

9 Configuration management

9.1 Overview

Configuration management is a key part of IDM that provides for assurance and sustainment of functionality and performance of applications which use intelligent devices. IDM configuration activities are a part of a larger management system for IACS configuration. IACS configuration is generally a large set of activities that are usually broken into parts to help manage complexity. However, all the parts are interdependent. Configuration management for IDM includes integration of intelligent devices into the IACS. Therefore, the configuration tools and work process become integrated as well.

Information is more than data. Information includes the following:

- data and metadata that can be stored in databases;
- how the device communicates;
- models that utilize the data and provide context and meaning to the data;
- graphical relationships;
- explanation and text including requirements, standards, guidelines, and other expressions of intent or decisions made;
- systems and tools that act on and/or manage the information;
- human resources necessary to understand, integrate, and manage the information in a manner that satisfies the needs of facilities.

9.2 Device templates for device configuration

Intelligent devices contain large numbers of parameters which, for example:

- define the identity of the device;
- identify the application where the device is used;
- define basic operational information such as measurement range;
- define any control actions required of the device;
- define schedule for activities;
- define diagnostics to warn of abnormal conditions, how these diagnostics will be presented, and to whom;
- define failure handling for the device and associated control processes.

The set of configuration parameters for an intelligent device can contain hundreds of parameters. All of these parameters need to be understood, organized and set by someone using an efficient and accurate process. Determining the proper settings for large numbers of parameters in the field during device commissioning is very inefficient. Work processes that use configuration interfaces that modify one parameter at a time are error-prone.

The process for managing these parameters starts with the creation of templates containing consistent sets of default settings for parameters. The template is supported by information describing what each parameter does, why the default was chosen, and when the default is changed for a particular device application. At least one template is needed for each type (model) of device.

New templates need to be created for each new device model that has new or changed parameters or options.

A minimum set of device templates is expected to be provided and maintained by the enterprise owning the facility collaborating with device vendors. There can be multiple templates for different common applications of a device (such as flow, level, or pressure measurement by a differential pressure device).

Typical configuration data sets, which need less modification than templates when they are replicated and used for individual applications, can also be used.

These templates and typical configurations are stored and managed as libraries for device configuration data. They support auditing of configuration management.

9.3 Toolkits

Intelligent devices are a part of systems and their configuration data need to be integrated with systems. Toolkits provide the typical configuration data management tools and work processes for integrating intelligent devices with systems. Both toolkits and templates are used for intelligent device configuration management.

Toolkits are normally maintained by the MAC and include the following:

- control strategies including automated fault handling;
- graphics and HMI configuration linked to control strategies;
- configuration tools and work processes.

Toolkits are valuable during facility implementation, project execution, and work processes that support IDM projects. However, toolkits do not provide the tools and work processes generally used by maintenance.

9.4 Configuring intelligent devices

9.4.1 Overview

There are two common processes for configuring intelligent devices. One is bulk building and the other is individual building.

9.4.2 Bulk building

Bulk building is used in large facility implementation projects to efficiently configure large numbers of devices offline. This work process uses typical configuration data exported from a host system, replicated and modified in configuration databases external to the host system, and imported back into the host system for later download to devices.

Bulk building is used typically in transition to the maintenance of large projects to efficiently configure large numbers of devices. The tools and skills used for bulk building are then preferred by facility implementation projects and not used by maintenance. The change in tools is further compounded by a change in personnel. This is because project personnel generally do not stay with a facility and provide support after project completion. The combination of new tools and new people can result in an unmanaged discontinuity in configuration management unless the transition is planned and managed.

9.4.3 Individual building

Individual build is normally done to configure a single device or control loop that is being added or modified. The process normally starts with a typical configuration that can be replicated and modified inside the host system for the particular application, checked, and then downloaded when needed.

When devices are replaced in kind (with an identical device) no configuration data modifications are necessary. A simple download suffices in most cases. However, device replacement with an unlike device (i.e. device of the same model but perhaps newer software/firmware version) can result in a loss of functionality, the opportunity to add new functionality, or simply a necessary configuration change to perform the same function. Whenever configuration or functionality change is needed, it is evaluated and carried out under management of change (MOC).

9.5 Maintenance of device configuration data

One of the problems with configuration management is that the same data is used by a number of independent applications – each supported by their own database. For instance, tag number, engineering units, and measurement range can be in the device, the control system, an engineering design tool, a process modelling system, a computerized maintenance management system, and more. Device data in the configuration database is stored in human readable versus machine readable parameter format.

When unintentional changes are made, those mistakes need to be corrected based on “master data”. When intentional changes (design changes) are made, the changes gradually propagate through all of the databases as the IDM project is implemented. Most current applications with a configuration database are built as if they own the master data record. Most have some ability to import or export data, but parameter name translation is needed to accomplish the import. Moving data from one database to another is a manual process, and keeping track of the data master at any point in time is also a manual process. The master set of data changes location as changes in projects are implemented and throughout the lifecycle.

Keeping configuration databases synchronized and accurate over the facility lifecycle is dominated by manual processes that are prone to human error. Some standardization and automation of this process can be beneficial. Audits are necessary to ensure long term data integrity.

Annex A
(informative)

Standard diagrams used in IEC 63082 (all parts)

A.1 Overview

ISO/IEC 19501, a unified modelling language (UML) specification, provides for structure diagrams and activity diagrams. The structure diagram called a class diagram and the behaviour diagram called an activity diagram (otherwise known as a swimlane diagram) are utilized in IEC 63082 (all parts). Class diagrams are used to explain some types of documentation. Activity diagrams are used to document work processes.

Figure A.1 shows the positioning of these diagrams among the UML diagrams.

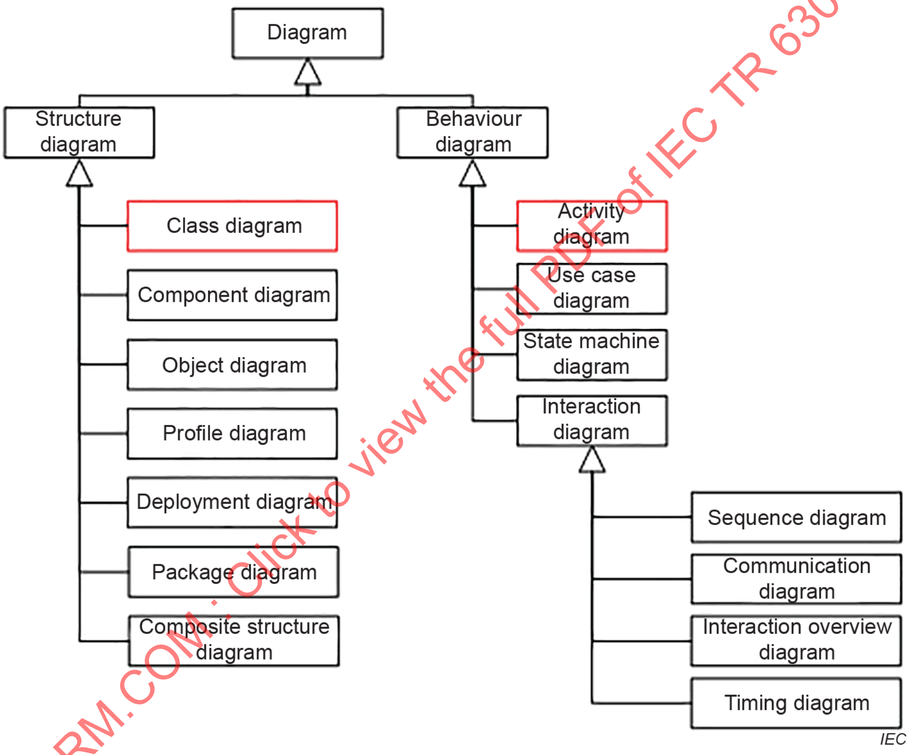


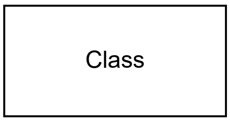
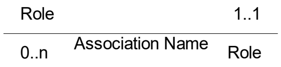
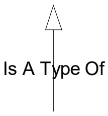
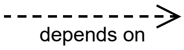
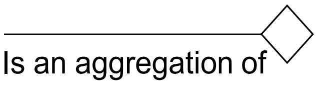
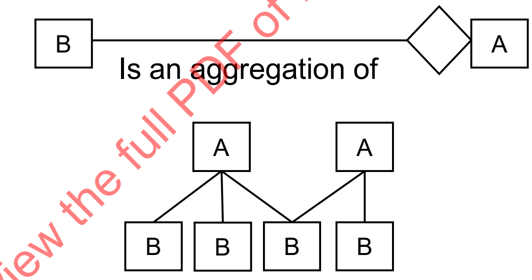
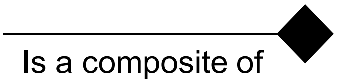
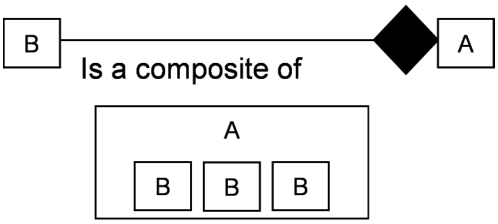
Figure A.1 – Position of class diagram and activity diagram in UML

A.2 Class diagram

Class diagrams show relationships and dependencies or ownership.

Table A.1 shows the notation of UML class diagrams used in this document while Figure A.2 shows an example of a class diagram. This notation follows ANSI/ISA-95.00.02-2018.

Table A.1 – Notation of UML class diagram

Symbol	Definition
	Represents a UML class of objects, each with the same types of attributes. Each object is uniquely identifiable or enumerable. No operations or methods are listed for the classes.
	An association between elements of a class and elements of another or the same class. Each association is identified. May have the expected number or range of members of the subclass, when 'n' indicates an indeterminate number. For example, 0..n means that zero or more members of the subclass may exist.
	Generalization (arrow points to the super class) shows that an element of the class is a specialized type of the super class.
	Dependence is a weak association that shows that a modeling element depends on another modeling element. The item at the tail depends on the head of the relationship.
	Aggregation shows that an element of the class is made up of elements of other classes. EXAMPLE 1  B Is an aggregation of A A A B B B B
	Composite shows a strong form of aggregation, which requires that a part instance be included in at most one composite at a time and that the composite object has sole responsibility for disposition of its parts. EXAMPLE 2 

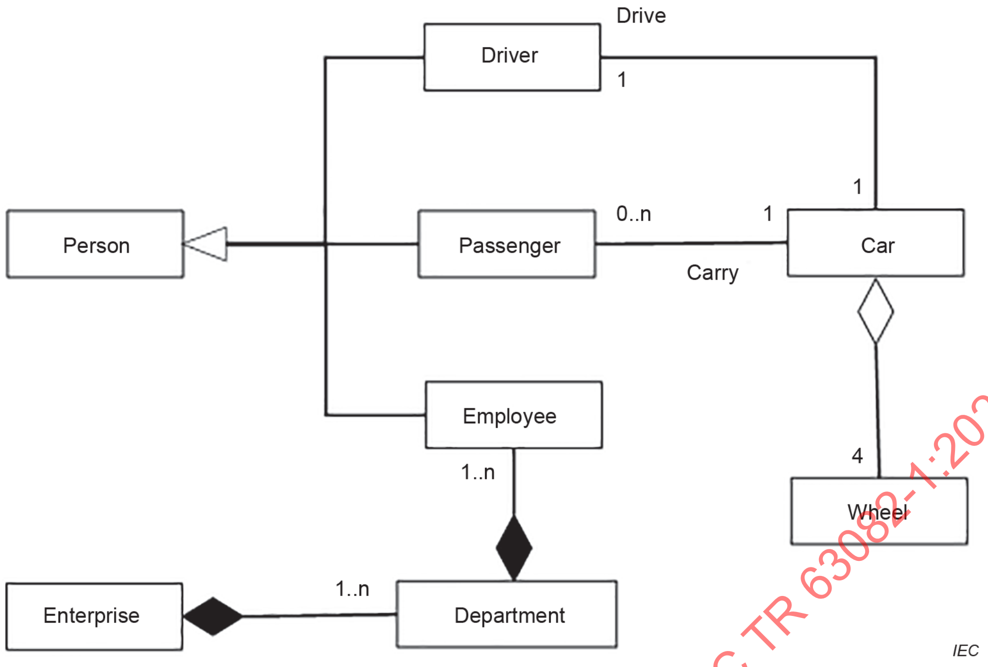


Figure A.2 – Example of class diagram

A.3 Activity diagram (swimlanes)

A.3.1 Overview

A swimlane chart is a derivation of an activity diagram. Swimlane charts are used to organize responsibility for actions and subactivities. They often correspond to organizational units in a business model.

Good models are essential for communication among project teams and to ensure architectural soundness. We build models of complex systems because we cannot comprehend any such system in its entirety. Having a rigorous modelling language standard is one essential factor. UML is one of those modelling languages.

UML is a graphical language for visualizing, specifying, constructing, and documenting the artefacts of a software-intensive system. The UML offers a standard way to write a system's blueprints, including conceptual things such as business processes and system functions as well as concrete things such as software programming language statements, database schemas, and reusable software components. The UML represents the culmination of best practices in practical object-oriented modelling.

A modelling language includes:

- model elements – fundamental modelling concepts and semantics;
- notation – visual rendering of model elements;
- guidelines – idioms of usage within the trade.

In Annex A, the following elements of the swimlane chart are described.

A.3.2 Activity diagram

An activity diagram is used to model processes involving one or more classifiers. Its primary focus is on the sequence and conditions for the actions that are taken, rather than on which classifiers perform those actions.

An activity diagram is a special case of a state diagram in which all (or at least most) of the states are action or subactivity states and in which all (or at least most) of the transitions are triggered by completion of the actions or subactivities in the source states.

Most of the states in such a diagram are action states that represent atomic actions, that is, states that invoke actions and then wait for their completion. Transitions into action states are triggered by events, which can be the

- completion of a previous action state (completion events);
- availability of an object in a certain state;
- occurrence of a signal;
- satisfaction of some condition.

An activity diagram defines a computational process in terms of the control-flow and object-flow among its constituent actions. It does not extend the semantics of state machines in a major way but it does define shorthand forms that are convenient for modelling control-flow and object-flow in computational and organizational processes.

The purpose is to focus on flows driven by internal processing (as opposed to external events). Use activity diagrams in situations where all or most of the events represent the completion of internally-generated actions (that is, procedural flow of control).

Table A.2 describes model elements of the activity diagram.

Table A.2 – Model elements of activity diagram

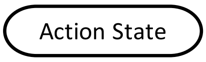
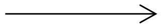
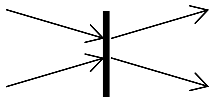
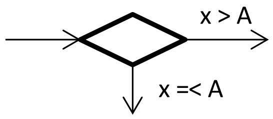
Name of element	Description	Notation
Action state	A shorthand for a state with an entry action and at least one outgoing transition involving the implicit event of completing the entry action (there may be several such transitions if they have guard conditions).	A shape with straight top and bottom and with convex arcs on the two sides. 
(Simple) transitions	A relationship between two states indicating that an instance in the first state will enter the second state and perform specific actions when a specified event occurs provided that certain specified conditions are satisfied.	A solid line originating from the source state and terminated by an arrow on the target state. 
Synchronization bar	A concurrent transition is enabled when all the source states are occupied. After a compound transition fires, all its destination states are occupied. The synchronization bar can represent synchronization, forking, or both.	A short heavy bar. 
Decision	An activity diagram expresses a decision when guard conditions are used to indicate different possible transitions that depend on Boolean conditions of the owning object. The icon provided for a decision is the traditional diamond shape, with one incoming arrow and with two or more outgoing arrows, each labelled by a distinct guard condition with no event trigger. The same icon can be used to merge decision branches back together, in which case it is called a merge.	Traditional diamond shape, with one incoming arrow and with two or more outgoing arrows, each labelled by a distinct guard condition with no event trigger. 

Figure A.3 is an example of activity diagram, which models the preparing of a beverage.