
**Security and resilience — Emergency
management — Guidelines for
monitoring facilities with identified
hazards**

*Sécurité et résilience — Gestion des urgences — Lignes directrices
pour la surveillance des installations à risques identifiés*





COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Monitoring	2
4.1 General.....	2
4.2 Monitoring process.....	2
4.3 Data characteristics.....	2
4.4 Data analysis and interpretation.....	3
4.5 Output.....	3
5 Implementing and operating the monitoring process	3
5.1 General.....	3
5.2 Planning.....	4
5.3 Implementation.....	4
5.4 Operation and control.....	5
5.5 Review and continuous improvement.....	5
Annex A (informative) Examples of facilities with identified hazards	6
Annex B (informative) Examples of possible hazards	7
Annex C (informative) Example of monitoring at a facility	8
Annex D (informative) Examples of decision support documents	10
Bibliography	11

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

In recent years, there has been a growing awareness of the risks and consequences of natural and industrial disasters. Monitoring hazards can reduce potential losses through improved prevention, mitigation, preparedness and a more effective response to incidents resulting from the hazards.

Effective monitoring can provide public and private sector emergency management with ongoing, timely, accurate, easily understood relevant monitoring data to support decision-making in emergency management.

Security standards are continually evolving and improving. Advances in monitoring technology will provide opportunities for further improvement of these guidelines and for development and application of innovative monitoring solutions.

The purpose of this document is to contribute to an overall emergency management framework which seeks to reduce the risk to people, operations, property and the environment.

This document provides guidelines for the entire process of hazard monitoring at facilities with identified hazards, including planning, implementation, operation and control, and review and continual improvement. This document is applicable to all facilities with identified hazards and may be used by stakeholders and authorities responsible for safety and security, such as

- owners and operators of facilities,
- engineers, installers and contractors during facility planning, construction, and maintenance,
- public authorities responsible for emergency prevention activities and incident response,
- insurance companies and potentially affected residents,
- legislators, and
- the scientific community and researchers.

Security and resilience — Emergency management — Guidelines for monitoring facilities with identified hazards

1 Scope

This document gives guidelines for monitoring hazards within a facility as a part of an overall emergency management and continuity programme by establishing the process for hazard monitoring at facilities with identified hazards.

It includes recommendations on how to develop and operate systems for the purpose of monitoring facilities with identified hazards. It covers the entire process of monitoring facilities.

This document is generic and applicable to any organization. The application depends on the operating environment, the complexity of the organization and the type of identified hazards.

2 Normative references

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

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

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

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

3.1

data analysis

systematic investigation of relevant, evidence-based information obtained in the monitoring process and its flow in a real or planned system

3.2

monitoring process owner

individual or legal entity responsible for receipt, integration, generation, analysis, transfer and output of data

Note 1 to entry: A monitoring process or owner of a system within the monitoring process can be represented, e.g. by a sub-contractor.

3.3

critical indicator

quantitative, qualitative or descriptive measure used to assess the hazard being monitored to identify the potential for the development of an incident, accident or emergency

Note 1 to entry: Critical indicators provide information about the most important integral characteristics of the structural state of a facility.

3.4 facility

plant, machinery, property, building, transportation units at sea/land/airport, and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function of service

Note 1 to entry: A facility can have formal boundaries as defined by, for example, legislation.

4 Monitoring

4.1 General

Monitoring should identify dynamic hazard development at facilities with identified hazards that can lead to incidents. This should include the provision of timely relevant and reliable data about the hazards.

NOTE 1 [Annex A](#) provides examples of facilities with identified hazards.

The selection of hazards to be monitored should be based on the results of the hazard identification and risk analysis.

NOTE 2 [Annex B](#) provides examples of possible hazards.

Monitoring should provide progressive notification as the incident escalates; at a minimum: normal, caution and emergency.

Monitoring should reflect administrative and organizational considerations. It should include hardware and software appropriate to the hazard to support the monitoring process described in [4.2](#).

NOTE 3 [Annex C](#) provides an example for monitoring a facility.

4.2 Monitoring process

The monitoring process involves receipt, integration, generation, analysis, transfer and output of data. The process involves the facility owner, authorities responsible for safety and security and other stakeholders interested in obtaining monitoring data.

The monitoring process should provide data to facility owners, authorities and stakeholders by using pre-established procedures for sharing the data.

The monitoring process should

- a) monitor hazards and critical indicators,
- b) include information resulting from human intervention in the facility's operation modes,
- c) provide continuous, reliable, trustworthy (independent from maintenance service of the facility), dynamic critical indicators applicable to the identified hazards,
- d) provide real-time data transfer on critical indicator changes,
- e) prioritize the use of automated and manually operated systems, and
- f) evaluate the results of related maintenance for possible improvements to the monitoring process.

4.3 Data characteristics

The monitoring process should ensure that data

- a) are accumulated at the facilities,

- b) have the agreed characteristics,
- c) are easily analysed and interpreted,
- d) are transmitted via secured channels, and
- e) are capable of being integrated to support decision-making.

4.4 Data analysis and interpretation

Monitoring should ensure data are analysed and interpreted to meet emergency management needs and display facility indicators in a prioritized manner to support decision-making. Data should be displayed such that the most recent relevant indicators can be easily identified.

NOTE [Annex D](#) provides examples of decision support documents.

Data should be displayed in a comprehensive and understandable format which may include

- a) text messages,
- b) graphics including those displaying dynamic processes,
- c) audible signals, and
- d) video.

Data should be displayed in a manner such that the most recent and the most relevant indicators can be easily identified by an automated system. For the purpose of continuous improvement of the monitoring system and improving overall preparedness, data should be analysed by using incident statistics and forecasting models.

4.5 Output

In the event of increased risks the results of the monitoring process should be shared with pre-identified authorities and stakeholders (see [4.2](#)). The stakeholders are identified during the development/improvement stage of the monitoring process.

The output should be provided in an appropriate format for the pre-identified recipients based on the increased level of risks.

The information should be transferred in reliable and redundant manner and should be verified by the stakeholders.

5 Implementing and operating the monitoring process

5.1 General

The monitoring process owner should develop agreements that describe the monitoring process and the interaction between the process owner and others involved in the process as described in [4.2](#).

This involves

- a) planning ([5.2](#)),
- b) implementation ([5.3](#)),
- c) operation and control ([5.4](#)), and
- d) review and continuous improvement.

5.2 Planning

When planning the monitoring system the monitoring process owner should

- a) obtain input from monitoring stakeholders (see [4.2](#)) to support the monitoring process development,
- b) consider applicable standards and industry codes of practice,
- c) create a project design for a hazard resistant monitoring system including the scope, objectives and process approval procedures, for the hazards being considered,
- d) ensure adequate capabilities and qualifications required for personnel who will design, implement and operate the monitoring system and process, and
- e) provide specialized training where required for personnel who will design, implement and operate the monitoring system to ensure the required capabilities and qualifications are met.

The monitoring process owner and authorities responsible for safety and security matters should

- agree on project design solutions for monitoring,
- provide the facility owner with the necessary technical requirements for monitoring development, ensuring the transfer of monitoring data outside of the facility, and
- agree on procedures for issuing progressive levels of monitoring results at a minimum of normal, caution and emergency notifications, so that pre-planned responses will be triggered.

5.3 Implementation

The monitoring process owner should implement, test and ensure approval of the system in accordance with plans developed in [5.2](#).

The monitoring process owner should

- a) ensure that the implementation is performed based upon an agreement between the facility owner and relevant entities,
- b) ensure that the monitoring is conducted based on agreed arrangements,
- c) conduct the commissioning, testing, and approval based on best practices and applicable requirements,
- d) ensure all senders and receivers of the data and the information from monitoring have interoperability,
- e) ensure appropriate security clearances and authorization to access and activate warning systems are obtained for personnel,
- f) develop necessary monitoring procedures, and
- g) make certain that everyone involved in the implementation of monitoring is adequately trained to perform their required tasks.

Once monitoring is implemented, the monitoring process owner should take measures to check the quality, performance and reliability of all equipment and authorized personnel involved in all aspects of the monitoring process.

Stakeholders and authorities responsible for safety and security matters should ensure the interoperability of sending and receiving monitoring data, including procedures on interaction on received monitoring data.

5.4 Operation and control

The monitoring process should be operated

- a) by the monitoring process owner, in accordance with the scope and objectives identified in [5.2](#),
- b) by personnel who meet the qualifications and training in accordance with their roles and responsibilities identified in [5.1](#),
- c) in accordance with operating procedures developed during the implementation process (see [5.3](#)), and
- d) in cooperation with authorities responsible for safety and security matters.

The monitoring process owner should evaluate and update the monitoring process, as necessary, based on

- changes in the hazard identification and risk analysis or pre-identified scenarios,
- any indication the monitoring process is not operating as designed, and
- the results of validation tests and exercises of components and the entire process.

5.5 Review and continuous improvement

The monitoring process owner should ensure the monitoring process is reviewed at planned intervals. The results of the review should be documented and provided to the monitoring process stakeholders.

This review should

- a) use an assessment methodology appropriate for the monitoring process,
- b) involve personnel with appropriate expertise,
- c) consider changes in hazard identification and risk analysis,
- d) consider organizational changes,
- e) consider the results of monitoring system operation, tests and exercises,
- f) assess monitoring activities on a regular basis to ensure that safety, security and emergency response objectives are met,
- g) use the assessment results in ongoing decision-making; for example, when determining whether to cease supporting the monitoring system during facility shutdown or when conducting risk reduction activities, and
- h) implement system improvements based on assessment results.

Annex A **(informative)**

Examples of facilities with identified hazards

The following are provided as examples of potential facilities with identified hazards:

- a) facilities with critically important infrastructure;
- b) facilities where hazardous substances are made, used, recycled, produced, stored, transported or disposed in amounts exceeding the established norms;
- c) aerospace infrastructure facilities;
- d) oil fields development facilities in sea shelves;
- e) main gas and oil lines, product pipelines;
- f) large industrial facilities;
- g) facilities for entertainment and sports, multipurpose offices and shopping centres, healthcare facilities and hotels.

Annex B

(informative)

Examples of possible hazards

The following are provided as examples of possible hazards:

- a) failures in technological systems operations;
- b) fire;
- c) failures in heat supply, heating, hot and cold water supply;
- d) failures in electricity supply;
- e) failures in gas supply;
- f) lifting equipment failure;
- g) unauthorized access;
- h) high levels of radiation; maximum allowed concentration of chemically hazardous substances; biologically hazardous substances; explosive concentrations of gas-air mixtures;
- i) flooding of premises, drainage systems and technological pits, resulting into possible disruption of life support systems and safety of facilities, and impeding evacuation of people and vehicles;
- j) gas leak;
- k) deviations from normative parameters of technological processes that could result in an incident;
- l) malfunction of emergency protection systems, safety and fire protection;
- m) changes in the state of engineering structures of buildings and facilities; engineering protection facilities;
- n) other natural events, such as earthquakes, high winds, tornados;
- o) other man-caused events, such as terrorist attacks.

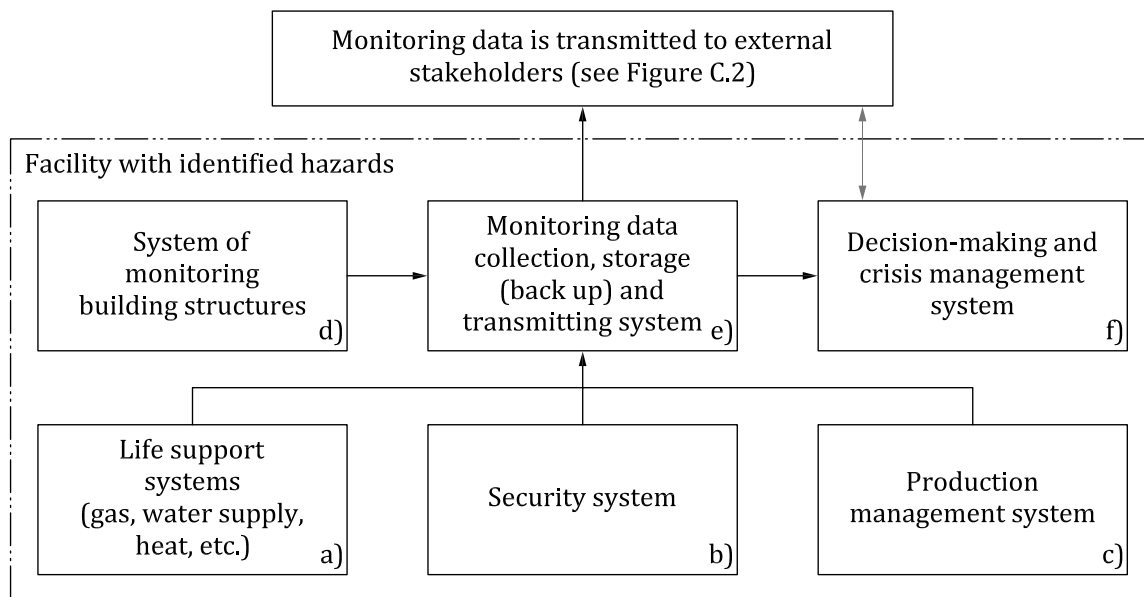
Annex C (informative)

Example of monitoring at a facility

A possible data structure of monitoring system at a facility with identified hazards is shown in [Figure C.1](#).

These data include the following.

- a) Monitoring data received from life support systems at a facility located in extremely cold climatic areas, which are very important for the safe operation of the facility.
- b) The status of security systems at a facility where hazardous substances are stored, which can become a critical indicator in identifying possible unauthorized distribution of hazardous substances outside the facility.
- c) Production management systems in a manufacturing facility, the indicators of which can also identify the possible development of incidents.
- d) A system of monitoring building structures, which, as a rule, is implemented on high-rise buildings, underground objects, large spanned bridges, etc. These systems monitor the structural condition of a facility and ensure control of the structural stability of a facility under high loads.
- e) Monitoring systems at a facility with identified hazards, which, depending on their purpose, may be present all at once or in various combinations, depending on the identified hazards.
- f) Data from all monitoring systems, which are collected, stored and processed within data collection and storage system, which is also a means of transmitting monitoring data to a decision-making and crisis management system.



Key

- automated process
- ↔ interoperability of specialists

Figure C.1 — The monitoring process at a facility

These systems enable the personnel of a facility to, and ensure that they can, make decisions on eliminating incidents in cooperation with both facility services and external stakeholders, see [Figure C.2](#).

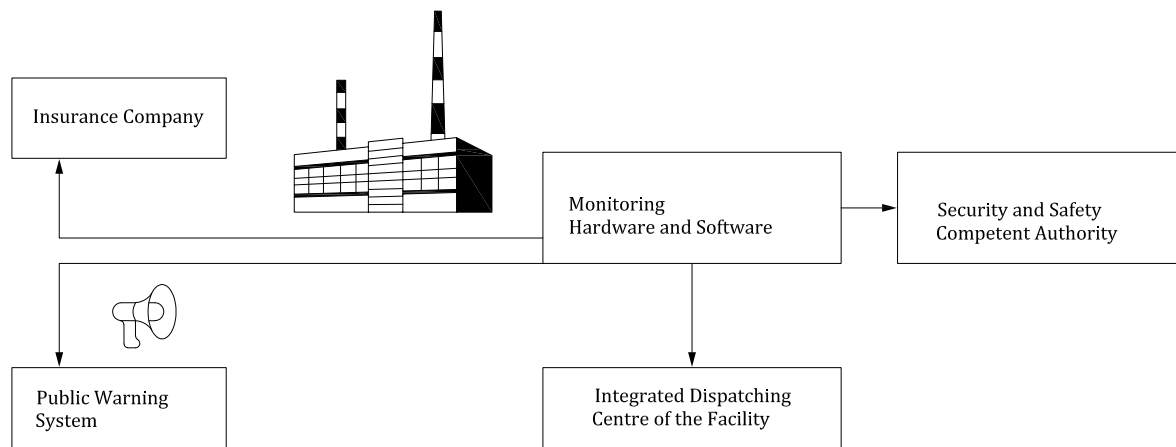


Figure C.2 — The process of monitoring of a facility connected to the authority responsible for safety and security matters

Annex D **(informative)**

Examples of decision support documents

The creation and display of messages about critical changes in monitored parameters, data collection and transferring functions can include the following:

- a) instructions for the monitoring process owner, corresponding to the displayed message;
- b) locations of registered incidents, accidents, fires and terrorist acts;
- c) diagrams of the facility, reflecting the current state of its main components;
- d) data, schemes, plans and reference information (on request), including the following:
 - 1) evacuation plans;
 - 2) location plans of main equipment and the state of engineering and technical support systems on the 3D model of the facility;
 - 3) facility entrance schemes;
 - 4) video data from the incident, accident or fire alarm location.

Bibliography

- [1] ISO 13824, *Bases for design of structures — General principles on risk assessment of systems involving structures*
- [2] ISO 22322, *Societal security — Emergency management — Guidelines for public warning*
- [3] ISO 22327,¹⁾ *Security and resilience — Emergency management — Community-based landslide early warning system*
- [4] ISO 28002, *Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use*

1) Under preparation. Stage at the time of publication: ISO/PRF 22327:2018.

