FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
24596**

ISO/TC **224**

Secretariat: **AFNOR**

Voting begins on:
2023-11-24

Voting terminates on:
2024-01-19

Drinking water, wastewater and stormwater systems and services — Guidelines for the planning and implementation of infrastructure hardening for water and wastewater systems

Reference number
ISO/FDIS 24596:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 Protection principles **2**
4.1 General 2
4.2 General objective for water infrastructure hardening 2
4.3 Main water and wastewater systems components 3
5 Risk assessment **3**
5.1 General 3
5.2 Vulnerability investigation 4
5.2.1 General 4
5.2.2 Site security plan 4
5.2.3 All hazards risk assessment 5
5.3 Asset risk categorization 6
6 Protective measures for infrastructure **7**
6.1 General protective measures 7
6.2 Security protection methods 7
6.2.1 General 7
6.2.2 Property protection by physical means 8
6.2.3 Monitoring and detection of intrusion 8
6.2.4 Property protection by human means 8
6.2.5 Security zones 9
6.2.6 Property protection by organizational means 9
6.3 Protection measure validation 9
6.4 Protection assessment 9
6.4.1 General 9
6.4.2 Ongoing review 9
6.4.3 Corrective measures 9
7 Documentation **9**
8 Infrastructure hardening examples and configurations **10**
8.1 General 10
8.2 Recommended configurations for the hardening of the different elements of a water system 10
Annex A (informative) **Example of recommended security measure configurations for water and wastewater infrastructure as practised in Israel** **11**
Annex B (informative) **Example of the indicative asset security categorization and security treatment schedules as practised in Australia** **14**
Annex C (informative) **Example of recommended security measure configurations for water and wastewater infrastructure as practised in Germany** **23**
Annex D (informative) **Example of general protection elements for water and wastewater infrastructure** **25**
Bibliography **30**

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).

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

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 224, *Drinking water, wastewater and stormwater systems and services*.

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

Hardening of water and wastewater infrastructure is one of the most crucial issues to address when formulating and implementing a plan for assuring the security of water and wastewater systems. The delivery of strong safety and security outcomes is essential to protect employees, the public and the assets of the water utility. Securing the assets and operations, where these facilities constitute an essential element of water service continuity or contain hazards or risks to the public, should be central to each water utility's safety and security programme and demonstrated through applied risk management principles, business activities and associated corporate documentation. These assets are crucial to ensure service continuity and minimize risks to the community.

Over the past few years there has been an increase in water and wastewater supply crisis events associated with:

— climate change;

— cyberattacks on water infrastructure;

— civil disruption;

— terrorist-related physical attacks on civil targets.

There has also been an increase in public awareness of water and wastewater incidents.

Under these circumstances, the protection of water and wastewater infrastructure is of critical importance.

Hardening of water and wastewater infrastructures has the aim of enhancing the protection of these infrastructures. Hardening consists of construction and creation of barriers, that can include physical and electronic elements, personnel and organizational measures, with the purpose of making it difficult to intentionally or unintentionally disrupt service continuity, supply and quality.

Examples of such barriers include fences, buildings, electronic alarms and cameras connected to control rooms, remote valves, both manual and remote controlled, backflow preventers, analysis software, such as event detection systems (EDS, as described in ISO/TS 24522)[1] and software designed to prevent cyberattacks.

Another type of protective system is the installation of monitoring equipment for water quality and operational parameters. This document only briefly refers to this type of protection. For more information, see ISO/TS 24541[2].

Drinking water, wastewater and stormwater systems and services — Guidelines for the planning and implementation of infrastructure hardening for water and wastewater systems

1 Scope

This document provides guidelines for the planning and implementation of hardening of different water and wastewater infrastructures aiming to improve the resilience of water and wastewater services provided by water utilities through security measures.

It applies to the determination of measures for the protection of water supply systems and sewer collection systems from unwanted or unplanned access, as part of risk management. This document is applicable to all water and/or wastewater utilities.

This document does not include guidelines for the protection of large water sources such as lakes or rivers.

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 24513, *Service activities relating to drinking water supply, wastewater and stormwater systems — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 24513 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
access point
opening or accessible opening in the perimeter of a site, building, structure or cabinet

3.2
alarm
audible and visual signal alerting a condition requiring immediate attention or user action

[SOURCE: ISO 8468:2007, 3.1.3[3]]

3.3
alarm response
type and timeframe of physical response to a designated site to enable an informed management decision in response to an *alarm* (3.2) or other alert

3.4
detector
item of electronic hardware which transmits designated signals (e.g. fire or movement) under specified environmental conditions to a control panel

3.5
integrate
conceptual and physical linkage between the planning aspects of protective monitoring systems

EXAMPLE Fire systems linked to intruder alarm systems and access control systems, with common interphase and signalling under prescribed conditions.

3.6
security
resistance to intentional acts designed to cause harm or damage

[SOURCE: ISO 28001:2007, 3.20, modified — the phrase "to or by the supply chain" was removed[4]]

4 Protection principles

4.1 General

Hardening of assets should be based on the following principles:

— risk-based approach;

— continuity and integration of water services;

— security and safety of the community and employees;

— assurance that appropriate standards and controls have mitigated risks inherent to water and wastewater infrastructure.

Hardening of water and wastewater infrastructure is divided into electronic and non-electronic, personnel and organizational measures, with the purpose of making it difficult to intentionally or unintentionally disrupt the service supply and cause the quality to deteriorate.

For initial security measures, a combination of physical measures (i.e. non-electronic measures) are often used – e.g. fencing or other entry barriers. Where the physical protection measures do not meet the required level of protection, electronic security measures should be used. In particular, physical property protective measures primarily refer to buildings and above-ground facilities or to buildings with above-ground access. As a rule, personnel and organizational measures are required for the property protection of underground assets.

The property protective measures should be based on a risk assessment approach and may also be staged based on the level of hardening required. Basic protective measures in the event of increasing danger should be supplemented by additional prevention measures, depending on the situation. These preventive measures may consist of personnel or organizational measures. Personnel measures are related to access control, patrolling and guarding. Organizational controls relate to, for example, employment and periodic safety visits and the conduct of exercises and post-security incident analysis.

4.2 General objective for water infrastructure hardening

Measures used to harden a water or wastewater facility should be conceived and revised in line with evolving national security risk advice, national security guidelines, legal risk determinations and local and regional risk conditions, as well as organizational and operational risk assessments.

The general objectives for the hardening of water infrastructure should be:

— preventing or delaying unauthorized access to water and wastewater assets, to avoid destruction or interference, creating the conditions for conveying to the relevant bodies immediate knowledge that someone may have accessed a water infrastructure without authorization;

— allowing the detention or identification of intruders and the initiation, if necessary, of subsequent prosecution by law enforcement.

4.3 Main water and wastewater systems components

The main water and wastewater systems components which should be considered for hardening purposes are:

— treatment plants and their components;

— water and wastewater reservoirs and tanks (open and closed);

— water abstraction and bulk water storage facilities, such as dams and groundwater wells;

— water supply off-takes and diversions;

— water and wastewater supply network infrastructure.

The application of risk-based benchmarked security and public safety principles and standards to the water and wastewater assets should be applied to achieve a cohesive protective security effect. The following key principles should be considered:

a) The levels of risk control should be determined using evidenced-based risk assessments.

b) Risk assessments should be benchmarked against infrastructure, community security and public safety risk experience.

Water utility managers should:

— identify the risk to public safety and security;

— monitor conformity with safety and security standards;

— operate and maintain assets in accordance with corporate requirements;

— ensure the applied public safety and security treatments are appropriate to the risk environment.

5 Risk assessment

5.1 General

To formulate a plan for the hardening of water system infrastructure, risk assessment of the system should be performed to decide which elements of the water system will be hardened and to what extent, and to establish a priority order of implementation.

The risk management plan should be developed in a manner consistent with ISO 31000.[5] In the development of a risk management plan, all stakeholders, including external regulators and institutions, should be identified. Accountability for the risk management plan development, delivery and review should be clearly designated.

To assist in developing the risk management plan, a system vulnerability investigation should be performed on all the elements of the system mentioned in 5.2.

5.2 Vulnerability investigation

5.2.1 General

A vulnerability investigation requires the development of a site security plan and undertaking of an "all hazards" review (see 5.2.2 and 5.2.3).

5.2.2 Site security plan

The site security plan should document the current conditions of the installation in relation to security.

The site security plan should:

a) document the layout (see ISO 24518[6] and ISO/TS 24520[7]) and site security aspects of the system or facility being secured, including items such as:

— water wells;

— tanks or reservoirs and other storage facilities;

— hydrants, accessories, pipelines and connections;

— open channels;

— water treatment plant components;

— wastewater treatment plant components;

b) note the requirements of relevant, occupational health and safety, environmental and security legislation;

c) identify specific requirements of the water utility, including provision for future expansion of the system and/or required augmentation to the existing system;

d) include critical details related to the "all hazards" risk management plan, including:

— impacts on the community (see ISO 24518[6] and ISO/TS 24520[7]);

— alternative drinking water, wastewater, stormwater and non-drinking water services;

— product quality performance requirements;

— quantity and reliability requirements;

— outcomes from the asset risk classification;

e) document the security profile of the system, including an assessment of the local environment and general area of influence, including:

— geography;

— meteorology;

— demography;

— emergency, police, security and medical response services;

— asset categorization of the site and its individual components;

— operations of the site;

— other equipment and assets;

— visible deterrence level required, versus the detection and response capacity available for the subject site;

— total loss effect, redundancy capacity, depth of contingency planning and repair capacity;

f) document engagement with key stakeholders, including government officials and the police, as deemed necessary by the water utility.

5.2.3 All hazards risk assessment

During the planning, concept and design phases of new, extended, upgraded and renewed water systems, a practical and appropriately documented “all hazards” risk assessment should be undertaken in accordance with ISO 31000.[5] To ensure effective property protection, a precise analysis and evaluation of hazards of both the individual infrastructure and the entirety of the water supply systems in accordance with risk management practices should be carried out on the basis of the protection objectives described in 4.2. This should include recurring and event-related hazards and consider the nature and extent of the hazard and its potential impact on the infrastructure (see Annex C).

Risk should be defined by the components of likelihood (plausibility) and consequence. In determining the consequence, the vulnerability of the infrastructure, including functional susceptibility and replaceability, should be taken into account.

The functional susceptibility includes aspects such as the dependence or effect on other internal and external infrastructure and the intrinsic robustness of the water infrastructure against external influences. Replaceability includes aspects such as redundancy and the expected effort to restore services. In addition to the direct effects on the infrastructure, the effects on the whole or parts of the water supply system should be determined and taken into account in the risk classification.

The “all hazards” risk assessment should qualitatively and quantitatively identify and assess the following risk areas, as a minimum:

a) environmental hazards;

b) external and internal human environment:

1) natural hazards, e.g. fires or floods;

2) human induced, e.g. vandalism, sabotage, terrorism (noting that this can require engagement with authorities such as the police to determine effectively);

3) geographic environmental risks:

   — proximity to population centres' direct and indirect risks to the population;

   — number of people served by the relevant system element;

   — supply to special type of users (e.g. hospitals, schools, key factories);

4) collateral systems and operational effects:

   — physical conditions of the system, e.g. accessibility, level of protection;

   — hydraulic nature of the system, e.g. gravity, pressure, open channel;

   — digital connectivity, e.g. manual operation, on-site automation, networked automation, centralized or distributed data collection;

   — operational, essential and emergency services and security response capabilities;

   — contingency bypass, replacement or recovery capability.

Following risk assessment, an appropriate and cost-effective level of hardening and asset protection should be determined for each asset category within the system using the asset risk categorization

(see 5.3). These appropriate protection components or required design features should in turn be incorporated into the final design of the infrastructure and reflected in the site security plan.

NOTE This approach assumes that consequence is the dominant variable in determining whether to harden a facility. The likelihood of an event can be of lesser significance than the consequence and is used to determine the aspects of the facility that require hardening. The reasoning is that if the potential consequence component of the risk is deemed high or medium, then even though the likelihood of an event is low, consideration must be given to hardening the installation. This is because the current environment of rapidly evolving threats, particularly terrorism and cyberattacks, coupled with customer expectations and reputational damage from successful attacks on this infrastructure area, means that compromise of the system is an unacceptable outcome.

5.3 Asset risk categorization

Asset risk categorization relates to the consequences of asset function loss. It provides a basis for selection of appropriate infrastructure protection treatments relevant to the impact on downstream water services during a period of disruption, taking account of the intrinsic ability to bypass the asset functionality and continue to deliver water services to achieve the required goals.

The water utility should define the asset categorization and the operational environment based on the risk assessment (implementing criticality analysis methods)[8].

A complex site (multiple functions and assets) may have an overall high rating with specific components receiving differing ratings, dependent on their criticality. In such cases, security of specific assets within a site perimeter should be considered as more practicable than treating the entire site.

Table 1 provides guidance on assigning the level of hardening relative to the impacts of loss of asset functionality.

Table 1 — Generic infrastructure protection guidance

Asset risk level	Description	Loss effect (impact)	Suggested hardening level
A	Critical operational site or component. Identified by external and internal stakeholders as critical for operation, loss effect, community perception and national defence or strategic requirements. Critical to the control and operational integrity of the integrated services or supply.	Community, commercial and industrial loss. Major contingency effort to continue operations. Major media and government attention, regulator investigation and potential action.	High
B	Key operational site. Key link in the integrated supply system. Significant or single source. May be remote with extended travel times or no local community. Located close to high-density population area. Essential supply link to important national defence or strategic asset.	Potential commercial and industrial loss for the community. Significant contingency effort to continue operations. Media and ministerial attention. Regulator investigation and potential action.	Medium
C	Operational site. Short effect. Or non-essential site. Minimal or no loss effect.	Minimal or zero commercial loss in the community. Limited or zero media attention. Regulator routine investigation.	Low

Once the desired level of security is determined, the outcomes from the risk assessment should be used to determine the necessity and priority for implementation of individual protective measures (see Annex A, Annex B and Annex C for examples).