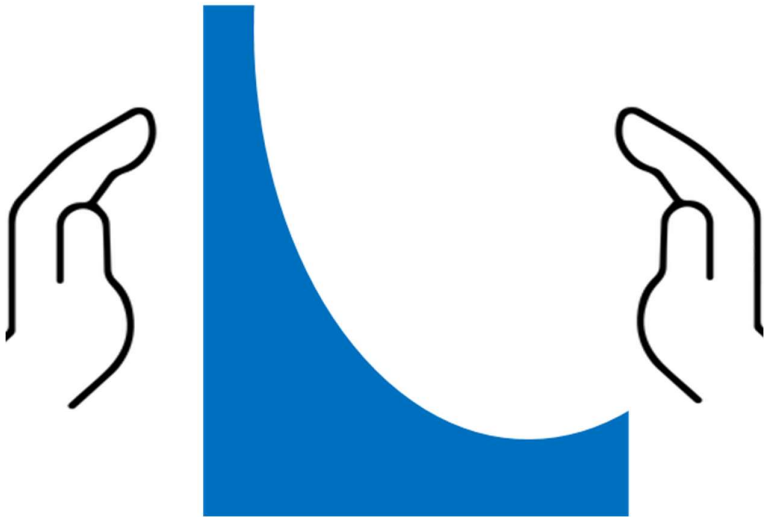

TECHNICAL GUIDE FOR THE PROTECTION OF STRATEGIC HYDRAULIC INFRASTRUCTURES

Disclosure version

2025

PROLOGUE

Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures (IICC), aims to establish the appropriate strategies and organizational structures that allow directing and coordinating the actions of the different bodies of public administrations in matters of protection of critical infrastructures.

This Law is developed by Royal Decree 704/2011 of May 20, which approves the Regulation of measures for the protection of critical infrastructures.

This state regulation defines Critical Operators as the entities or organizations responsible for the operation of the IICC, which in the Strategic Water Sector were designated in September 2015.

These Critical Operators must prepare a Specific Protection Plan for each Critical Infrastructure, for which they have a Guide of good practices prepared by the Security Secretariat of the Ministry of the Interior.

However, there is no guide for the world of dams that addresses this challenge from an engineering point of view, establishing failure modes, not only for physical and cyber security, but also involving structural safety.

This "*Technical Guide for the Protection of Strategic Hydraulic Infrastructures*" published by the Spanish National Committee for Large Dams, aims to support Operators in the design of protection measures for their infrastructures.

There are two versions of this guide, a complete one for operators and a shortened one for informational purposes. The version contained herein corresponds to the second one and for security reasons its content has been restricted.

The following members of the Spanish National Committee on Large Dams have participated in the preparation of this Guide:

Gómez López de Munain, René. (Director).

Echeverria Garcia, Eduardo. (Technical Secretary).

Castillo Rodríguez, Jessica Tamara.

De Cea Azañedo, Juan Carlos.

Domínguez Domínguez, María.

Escuder Bueno, Ignacio.

Garcia del Valle, David.

Gómez de Membrillera Ortuño, Manuel.

Gonzalez Tejada, Ignacio.

Granados Garcia, Alfredo.

Navarro Carrasco, Oscar.

Olalla Maranon, Claudio.

Red Martinez, Eduardo.

Although all members have reviewed the entire content of the guide, each chapter has been coordinated by one or more members, according to the following relationship:

Historical cases	Rene Gomez Lopez de Munain.
Access control failure	Eduardo Echeverría García.
Physical access cut off	Alfredo Granados García and David García del Valle.
Drone attack	Maria Dominguez Dominguez.
Eduardo Rojo Martínez's own personnel .	
Malicious activation of floodgates	Jessica Tamara Castillo Rodríguez and Ignacio Escuder Bueno.
Blasting or serious damage	Ignacio Gonzalez Tejada and Claudio Olalla Maranon.
Sabotage of the drainage system	Manuel Gómez from Membrillera Ortuño.
Cybersecurity/cyber-physical risks	Óscar Navarro Carrasco.
Intentional water pollution	René Gómez López de Munain.

I sincerely thank all members of the Strategic Hydraulic Infrastructure Protection Committee for their efforts and dedication in making the preparation of this Guide possible, which we hope will be useful.

Carlos Granell Ninot

President of the Spanish National Committee for Large Dams (SPANCOLD)

INDEX

INDEX OF ILLUSTRATIONS

1 INTRODUCTION

The essential services provided to society rely on a series of management infrastructures, both public and private, whose operation is essential. Thus, **Strategic Infrastructures** are the facilities, networks, systems and physical and information technology equipment on which the operation of essential services is based.

If these strategic infrastructures do not allow alternative solutions, they are called **Critical Infrastructures (IICC).**

For the purposes of this classification, hydraulic works are included in the Strategic Water Sector and may include infrastructure such as distribution networks, canals, water treatment plants, dams and reservoirs, etc. Their disruption or destruction would have a serious impact, which is why it is necessary to design a homogeneous and comprehensive security policy to protect them.

This was understood after the devastating effects of the Second World War, when in the First Protocol additional to the " ***Geneva Conventions of 1949*** " relative to the " *protection of victims of international armed conflicts* " of 1977, a specific mention is made of dams in its article 56 on Protection of works and installations containing dangerous forces and which is reproduced below:

" *1. Works or installations containing dangerous forces, namely* ***dams, dikes*** *and nuclear power stations,* ***shall not be subjected to attack, even if they are military objectives*** *, when such attacks may cause the release of those forces and consequently cause significant losses to the civilian population. Other military objectives located on or near such works or installations shall not be subjected to attack when such attacks may cause the release of dangerous forces and consequently cause significant losses to the civilian population.*

Following the Madrid attacks of 11 March 2004, the European Council approved the European Critical Infrastructure Protection Programme (ECIP) and launched a critical infrastructure alert information network.

Spain began its foray into the protection of Critical Infrastructures with the creation of the first National Plan for the Protection of Critical Infrastructures, on May 7, 2007, and the preparation of the first National Catalogue of Strategic Infrastructures grouped by sectors.

Subsequently, the Member States of the European Union developed Council Directive 2008/114 of 8 December on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. This Directive establishes that the primary and ultimate responsibility for protecting European critical infrastructures lies with the Member States and their operators, and determines the development of a series of obligations and actions to be carried out by each country.

For the same purpose, the Spanish government developed Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures, which aims to establish the appropriate strategies and organizational structures that allow directing and coordinating the actions of the different bodies of the public administrations in matters of protection of critical infrastructures.

This Law is developed by Royal Decree 704/2011 of May 20, which approves the Regulation of measures for the protection of critical infrastructures.

This state regulation defines Critical Operators as the entities or organizations responsible for the operation of the IICC, which in the Strategic Water Sector were designated in September 2015.

According to current regulations, the Operator must prepare a Specific Protection Plan (PPE) for each of the critical infrastructures, within four months from the approval of the Operator Security Plan (PSO). This is the operational document where the specific measures already adopted and those that the operator is going to adopt to guarantee the comprehensive security (physical and logical) of each of its critical infrastructures must be defined.

The Secretary of State for Security established, through the National Centre for the Protection of Critical Infrastructures by Resolution of 8 September 2015, the "*Minimum Contents of the Specific Protection Plan*", which all PPE must have, as well as the model on which to base its structure and completion.

Subsequently, the State Secretariat for Security published the "*Guide to Good Practices for the Specific Protection Plan*", a voluntary document that does not include additional requirements to those established by current legislation, with the intention of facilitating the application of these good practices.

The purpose of this Guide, in compliance with the previous documents, is to develop two essential aspects of the Specific Protection Plan applicable to the IICC, but which also has a place in the Strategic Hydraulic Infrastructures:

- The analysis of risks, especially the threats considered, relating them to the failure modes of the infrastructure.
- The protection measures (organizational, operational or technical) to be implemented in the infrastructure.

It is undeniable to admit that, although the approach of the treatment covers all hydraulic infrastructures, the professional bias of the authors makes the regulatory infrastructures a primary consideration.

2 DEFINITIONS OR GLOSSARY

Below we will describe some terms and acronyms used in the document, whose definitions must be clarified in order to have a correct understanding of the Guide.

a) Critical asset

Those resources, elements and systems of an infrastructure that are essential and indispensable to maintain and develop its capabilities and operation, or that are intended to fulfill that purpose.

b) Risk Analysis.

Study of possible threat hypotheses, necessary to determine and assess the existing vulnerabilities in the different strategic sectors and the possible repercussions of the disruption or destruction of the infrastructures that support them. (Source: Article 2 of Law 8/2011, which establishes measures for the protection of critical infrastructures). Section 5.2 lists the different assets and threats that are included in the risk analysis.

c) Strategic infrastructures

The facilities, networks, systems and physical and information technology equipment on which the operation of essential services is based. (Source: Article 2 of Law 8/2011, which establishes measures for the protection of critical infrastructures).

d) Critical infrastructures

Strategic infrastructures whose operation is essential and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services. (Source: Article 2 of Law 8/2011, which establishes measures for the protection of critical infrastructures).

e) Failure mode

A particular sequence of events that may lead to improper operation of the dam-reservoir system or a part thereof. This series of events is associated with a particular stress scenario and has a logical sequence, which consists of an initial triggering event, a series of development or propagation events and culminates in the failure of the dam.

Depending on the scope and objective of the analysis, the definition of the failure mode can be restricted to those that potentially involve the loss of human life or include any failure mode with the potential to produce an uncontrolled discharge of flows and therefore with the potential to cause damage of any kind (economic, to human life, the environment, etc.) and even any mechanism that causes some kind of damage (even without the need for a discharge to occur), for example one that causes economic consequences due to loss of mission. Likewise, the analysis of failure modes is not limited exclusively to the retention structures of a reservoir, but takes into account any element included in the dam-reservoir system. (Source: Technical Guide to Dam Safety No. 8: Risk analysis applied to the safety management of dams and reservoirs).

f) Risk

Combination of the probability of an event occurring and its possible negative consequences for human health, economic activity, the environment, infrastructure, cultural heritage, etc.

Risk = Hazard * Exposure * Vulnerability = Σ[P(Event)*P(Consequences) *P(Damage)]

In the world of dam engineering, the term “failure mode” is most frequently used, as the same threat can affect several failure modes. For example, a massive attack with explosives can produce two failure modes: damage to the gates and damage to the dam body. Section 5.1 describes a methodology for calculating and classifying them based on their impact and probability of occurrence.

g) Dangerousness

Hazard, danger or threat: probability of occurrence of a potentially damaging natural or anthropogenic event or sequence of events. It is the inverse of the Return Period. A list of the most frequent threats appears in Annex I.

h) Exposure

Description of the damage or consequences that a threat causes to the population, buildings, civil engineering works, economic activities, public services, environmental elements and other uses of the exposed territory.

i) Vulnerability

Probability of occurrence of the above damages.

j) Inherent Risk Level

Determines the level of risk that an asset or infrastructure has in the study situation.

k) Residual Risk Level

Level of risk that persists once the controls or security measures to mitigate the risks have been considered, thus determining the effectiveness of the measures implemented.

l) Sabotage

Destruction, damage, or manipulation that is intentionally done to an infrastructure, installation, service, process, etc., with the intention of causing serious harm, social alarm, fear, discredit, etc., as a form of struggle or protest in political, social, labor, or economic conflicts against the organization (body or company) that runs it, or as a method to benefit a person or group.

Types of Sabotage:

- **Physical**. Destruction, manipulation or alteration of the components of an infrastructure or its facilities, which causes direct or indirect damage to the infrastructure, workers or society.
  This sabotage is punishable by the Criminal Code. LO 10/1995, of November 23, articles 263 and 265: “damage to property of public or communal domain or use, ruining the injured party or placing him in a serious economic situation, use of poisonous or corrosive substances, infection or contagion of livestock.”
  Article 346 of the Criminal Code is even more explicit for infrastructure: “destruction of airports, ports, stations, buildings, public premises, warehouses

containing flammable or explosive materials, communication routes, means of collective transport, or the immersion or grounding of a ship, flooding, explosion of a mine or industrial installation, lifting of the rails of a railway, blowing up a bridge, destruction of a public road, damage to oil pipelines, serious disturbance of a means of communication, disturbance or interruption of the supply of water, electricity, hydrocarbons".

- **Cyber**. Conduct aimed at deleting or modifying functions or data in a computer application without authorization, to take unauthorized control of the device, hinder its correct operation, obtain information, cause damage to the hardware or software of the system, etc.
  These acts are punishable according to the Criminal Code. LO 10/1995, of November 23, article 264: "any means that destroys, alters, renders useless or in any other way damages data, programs or electronic documents belonging to others contained in networks, media or computer systems."
- **Informative or reputational** propaganda to discredit a person, organization or institution with the intention of damaging its image. In the private sphere, there is the right to civil protection of the right to honor, personal and family privacy and one's own image (Organic Law 1/1982, of May 5), and in the business sphere it is called Unfair Competition and is penalized by article 38 of the Constitution. In the public sphere, however, it is not penalized; in Spain there is no crime of "social alarm".
  This sabotage includes the so-called "disinformation campaigns", mainly through digital networks and press, where by creating "fake news" with a credible appearance, or spreading opinions that become proven facts, they spread them virally on the network, manipulating reality, or redirecting opinions. When the possible denial reaches the networks, the attackers have already managed to create the climate conducive to their objectives.
- **Sanitary**. It is the unauthorized act, where one seeks and intends to damage or destroy, sanitary facilities or services of public or private origin, and the contamination of air, water, or substances, the alteration or manipulation of medicines, food products for illicit purposes.
  It is punishable under the Criminal Code. LO 10/1995, of November 23, articles 359 and following: "anyone who produces substances harmful to health or chemical products, medicines, foods that may cause damage, or dispatches or supplies them, or trades in them, etc."
- **Social**: act of sabotage in which a large group of people is involved to fulfill a non-legalized demand.
- **Terrorist**. Indiscriminate threat or action from an organized group with the main intention of instilling terror through coercion, intimidation, harm or putting people, property or infrastructure at risk.
- **Warlike**. Violent actions of one nation against another carried out by military forces.

3 HISTORICAL CASES

Although sabotage in the world of water has not been one of the sectors most used to achieve dishonest ends, the future will bring us less availability of the resource as a consequence of population growth and climate change, and surely a worsening of its quality, which will undoubtedly encourage malicious acts.

Below are some examples of how the water sector, and dams in particular, have been used for violent purposes.

- Physical Sabotage.

- Itoiz Dam (Navarra, Spain 1996). After beating and tying up a security guard, eight saboteurs cut the steel cables of the concrete lathing of the dam, causing losses valued at more than 12 million euros at the time.

Illustration 1Sabotage of the Itoiz dam's dam cable (Navarra).

- Hat Gyi Dam (Burma, 2005). An unidentified group kills a Thai engineer during the construction of the dam on the Salween River in Karen State.
- Elche Dam (Alicante, Spain 2008). Unknown persons open the bottom drain gate, causing one million cubic metres of water and mud to flow out of the reservoir.
- Baksan Hydroelectric Power Station (Russia, 2010). Gunmen kill two workers at a hydroelectric power station and blow up its two turbines

- Cybernetic. In 2019, the National Cryptologic Centre (CCN) and the National Institute of Cybersecurity (Incibe) of Spain recorded more than 150,000 cybersecurity incidents involving companies, individuals and academic centres. Below are some cyberattacks in the water sector:

- Year 2000. Maroochy (Australia). A former employee dismissed by his company uses his knowledge to access the systems of a wastewater treatment plant and discharge untreated water.
- 2011. Springfield (Illinois, USA). An attacker operating from an IP address in Russia gains access to the SCADA system of a city water treatment plant and performs actions that result in the destruction of one of the infrastructure's pumps. (First confirmed cyberattack against a critical U.S. infrastructure.)
- Year 2013. Iranian hackers infiltrate the control system of a dam located just 25 miles from New York City, convincing the White House to double efforts to speed up U.S. defenses against cyberattacks.
- Year 2016. There is illegal access to the SCADAS of the Navarra Canal (Spain) and it is disseminated on the Internet.

  - News. Examples could include “Disinformation campaigns”, interference or manipulation in the 2016 United States elections, the 2016 Brexit elections, or the 2017 Catalan crisis. Also sensationalist journalistic information, for example “Pesticide in Aragonese water, the Spanish Chernobyl”, or “The rupture of the Yesa dam would submerge half of Zaragoza under 7 meters of water” (Spain, 2016)

  - Social

- Year 2020. Mexican farmers ambush hundreds of state soldiers guarding the La Boquilla dam in Chihuahua, Mexico, amid a dispute over water on the border with the United States. The Mexican government was sending water to Texas in compliance with the international treaty and, according to the farmers, it left almost nothing for their crops. The attackers took over the hydroelectric plant, causing damage valued at 4 million euros that took three months to repair and preventing the flow of water to the United States.

  - Sanitary.

- Year 1972. The Neo-Nazi Group "Order of the Rising Sun" attempts to poison the water in Chicago, St. Louis, and other cities in the American Midwest, with Typhus bacteria, attacking the distribution systems.
- Year 1973. A German biologist tries the same with anthrax and botulinum toxins in exchange for $8 million.
- Year 1983. Attempt to poison the water of Galilee.
- Year 1985. The extremist group "The Convent, the Sword and the Arm of the Lord (CSA)" attempts to poison the water distribution systems of New York, Chicago and Washington with potassium cyanide.
- Year 1992. Lethal concentrations of potassium cyanide are detected in the water storage tanks of an air base in Istanbul (PKK, Kurdistan Workers' Party).
- Year Four men arrested in Rome in possession of chemicals and detailed maps of the US Embassy Area supply network.

- Year 2002, USA. Two Al Qaeda agents arrested in Denver with plans to poison water supplies.
- Year 2004, USA. The FBI and the Department of Homeland Security say that terrorists were trying to recruit water plant workers.
- Year 2006, England. A water tank in Tring (England) was contaminated with herbicide.
- Year 2006, Denmark. Strychnine is poured into a Danish reservoir.
- Year 2007, China. 201 people die when water contaminated with fluorethamide was used.
- Year 2008, USA. In Varney (Virginia) a man was arrested with two bottles of cyanide to poison the water supply.
- 2008, Thailand. The water supply of a refugee camp in Thailand, with a population of 30,000 people, was intentionally poisoned with herbicide.
- 2009, Philippines. The Moro Islamic Liberation Front (MILF) of the Philippines poisoned water sources that were being used by government soldiers and the population.
- 2010, India. In the Kashmir region (India), Maoist rebels poisoned a pond used as a source of drinking water by the Central Reserve Police Force, a paramilitary group.
- 2010, England. A neo-Nazi couple was found guilty of manufacturing ricin and conspiring to poison water supplies used by Muslims.
- 2011, Spain. In La Línea de la Concepción (Cádiz, Spain), a plot was discovered to poison water supplies in response to the death of Osama Bin Laden.
- 2012, Australia. Two 5,000-litre drinking water tanks were deliberately poisoned in Diuron.
- 2012, Afghanistan. Hundreds of girls at a school fall ill when the water supply is intentionally poisoned.
- Year 2020, China. The coronavirus, with millions of infected people, has become a global pandemic. Although it is not transmitted through water, it has served to quantify the effects and consequences.

    - Terrorist.

- Panauti Plant and Seleghat Dam (Nepal 2001 and 2004). Maoist dissident groups blow up two hydroelectric plants.
- Kajaki Dam (Afghanistan, 2003 and 2008). The terrorist group ISIS launches three rockets and explosives at the dam, killing 11 British soldiers.
- Haditha Dam (Iraq, 2015). ISIS terrorists launch 7 car bombs at the Haditha Dam, killing 20 attackers.

Illustration 2Photograph of the Haditha Dam

- Pakistan, 2015. At least 20 workers are killed by a separatist group while working on the construction of an army-backed dam in the province of Balochistan in southwestern Pakistan.
- Mosul Dam (Iraq, 2016). Italian troops under UN mandate guard the Mosul Dam (Iraq) which is in danger after a "specific and detailed" threat of an attack by ISIS militants. They said the attack would be "the biggest ever conceived by the Caliphate" in Iraq. It will be "a large-scale assault that they have been working on for months."
- Salma Dam (Afghanistan, 2017). Taliban kill 10 security guards.

Illustration 3Photograph of the Salma Dam (Afghanistan)

    - Warlike. This is by far the one with the most data.
- During the Spanish Civil War (1936-1939) at least the following dams were affected:
    - Pena (Teruel). Republican troops blew up the Fondo Drains, breaking the safety and regulation gates and abruptly emptying the dam.

- Santolea (Teruel). Republican troops blew up the regulating gates of the bottom drain without affecting the safety gates. They also blew up the spillway bridge.
- Barasona (Huesca). The coup troops wanted to blow up the bottom drain, but the Manager convinced them that it was easier to open the drain gates and so they did.
- Ordunte (Burgos). Republican troops unsuccessfully attempted to blow it up by detonating 2,500 kilos of dynamite at the top.

- The most numerous cases were found in World War II:
  - Dnieprostroi (Russia, 1941). The Red Army made a 10m x 120m breach by placing 20 tons of ammonal in the hydroelectric dam, producing a flood wave that extended from Zaporizhia to Nikopol, killing local residents as well as soldiers on both sides. Historians estimate the number of victims to be between 20,000 and 100,000.

Illustration 4Photograph of the breach in the Dnieprostroi dam (Russia, 1941).

  - Dnieper (Russia, 1941) retreating Red Army troops demolish the dam and strategic hydroelectric power station with dynamite after the German invasion of the Soviet Union

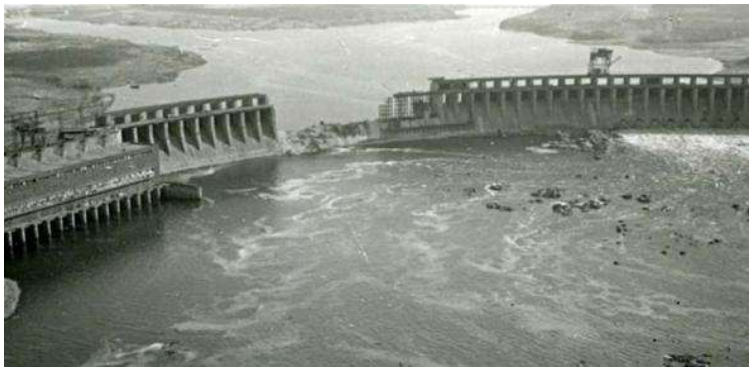

Illustration 5Breach of the Dnieper Dam (Russia, 1941).

- Dambusters During World War II, the British army devised a plan to demolish the German dams (Möhne, Eder, Sörpe) using bouncing bombs that moved over the surface of the reservoir water. Other attempts were made, such as Ennepe, but were unsuccessful. The Dambusters were 16 Lancaster bombers from Squadron 617, created specifically to destroy the German industrial centre (energy, factories in the Ruhr and railway infrastructure).

Illustration 6Möhne Dam (Germany, 1943). This dam had anti-aircraft guns and four attacks were necessary for its demolition.

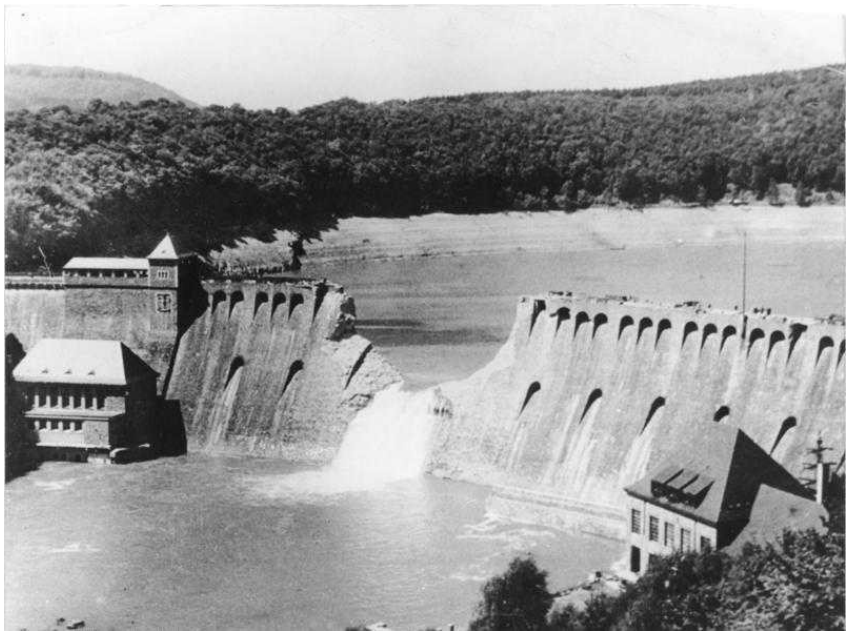

Illustration 7Eder Dam (Germany. 1943). The English attack took place on May 15, 1943, but despite the lack of anti-aircraft defenses, it was not easy due to its complicated topography with a strong wedging of the dam, needing three attempts to break it.

Illustration 8. . Sörpe Dam (Germany, 1943). Despite the crater-like depressions observed in the loose material dam, it was not breached due to anti-aircraft defences, difficult topography and fog.

- During the Korean War
    - Hwachon (South Korea, 1951). The 78 m high concrete gravity dam with a 435 m crest length was built by Japan during World War II. On May 1, 1951, the US 19th Air Group bombed the dam from eight Skyraiders, launching 7 MK13 torpedoes, of which six exploded, causing the breakage of two gates and damaging the third.

Illustration 9Hwachon Dam (South Korea, 1951).

- Sui-ho (South Korea, 1952). The Suiho complex was built by the Japanese in 1940 during World War II. It had the world's six largest turbines of 100,000 kW and a reservoir capacity of 20 hm3. It was the main source of electricity for the Soviet bases at Port Arthur and Dalian (present-day China), and the Russian port of Vladivostok in Siberia. On June 24, 1952, the American army attacked the power stations and transformers at the base of the dam.

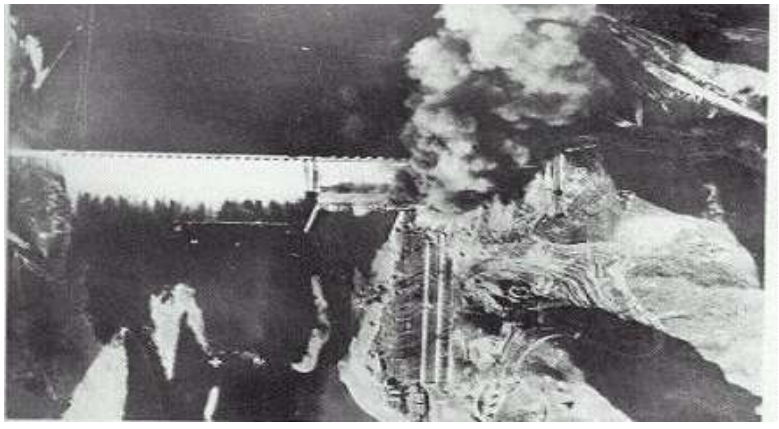

Illustration 10Sui-ho Dam (South Korea, 1952).

- Balkan war
  - Peruça Dam (Croatia, 1993). Loose-bed dam with a crest length of 425 m and a height of 60 m, built between 1955 and 1960. Serbian forces

placed 20 to 30 tons of TNT in five locations in the spillway and inspection gallery, but these were not sufficient to cause the dam to fail.

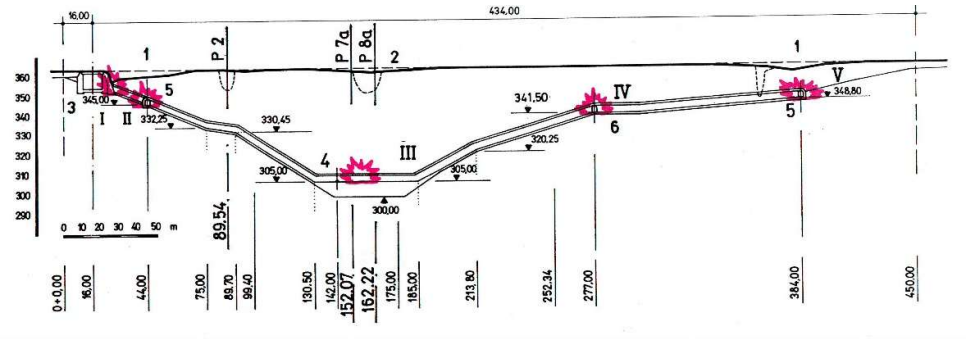

Illustration 11Placing explosives at the Peruca Dam (Croatia).

Illustration 12Photograph of the effects of explosives on the crest of the Peruca dam and spillway (Croatia).

- Ukrainian war
    - In June 2023, the Ukrainian Kakhovka Dam was destroyed by Russia, resulting in significant humanitarian and environmental consequences. The dam breach caused water levels to rise by up to 5 metres in the Kherson region, flooding at least 30 villages, affecting around 42,000 people and evacuating around 2,500 people on the Ukrainian-controlled shore.

Ilustration 13. View of the destruction of the Ukrainian Kakhovka dam.

4 DANGERS OR THREATS TO INFRASTRUCTURE

As previously described, within the framework of this guide, danger, hazard and threat have the same meaning. Structural safety failures of the infrastructure are excluded because they exceed the limits of this Guide.

An extension of the Threats is presented in Annex No. 1.

Two divisions are established: Global threats that can affect any infrastructure and Specific threats that only affect dams and reservoirs, or do so in a different way:

A. GLOBAL THREATS

1. Meteorological risks
   - Floods and floods
   - Fires
   - Thunderstorm
   - Electromagnetic pollution
   - Hurricanes and tornadoes
   - Heat wave
   - Cold snap
   - Extreme drought
   - Extreme ice, snow

2. Geophysical risks
   - Earthquakes
   - Landslides
   - Sinkholes or sinkholes
   - Volcanic eruptions
   - Geomagnetic storm

3. Terrorism and organized crime
   - Explosives in suicidal people
   - Explosives in manned ground vehicles
   - Explosives in unmanned ground vehicles
   - Explosives in unmanned aircraft
   - Explosives in boats or unmanned vessels
   - Explosives in boats or manned boats
   - Explosives in stopped vehicles
   - Explosives in packages sent by mail
   - Explosives placed or abandoned

- Grenade/mortar launcher attacks
- Armed terrorist attack
- Mass poisoning
- Chemical attack
- Radiological attack
- Biological attack
- Nuclear attack
- Arson
- Electromagnetic pulse

4. Aggressive crimes
   - Assault and extortion
   - Sabotage
   - Bomb threat

5. Ordinary crime
   - Heist
   - Theft
   - Fraud
   - Vandalism
   - Illegal Occupation

6. Cybernetic

B. PARTICULAR THREATS

1. Malicious Physical Failure
   - Cutting off physical access to the infrastructure.
   - Malicious power outage, telephone, communications, etc.
   - Intrusion into facilities preventing control of them.
   - Malicious activation of floodgates (spillways, bottom drains or intakes) or breakage of pipes.
   - Obstruction or introduction of foreign elements into the aeration ducts of valves and gates, manholes of pipes, etc.
   - Destruction of gate drive panels.
   - Blasting or serious damage to dam elements.
   - Handling drainage in factory dams
   - Intentional contamination of stored water or supply networks.
   - Intentional contamination of the air in galleries or chambers.
   - Use of drones with explosives or contaminants.
   - Intentional sabotage by the organization's own personnel
   - Targeted attacks (spoofing, abuse, repudiation, destruction, etc.)

2. Cyber-physical systems failure
    - Interference in monitoring software resulting in the inability to view the current status or act through the system's human-machine interfaces: Encryption of real-time servers, unauthorized access to monitoring or management interfaces…
    - Interference in network and communications electronics resulting in, for example, loss of communications, modification of network settings, etc.
    - Interference in communications for the purpose of, for example, representing false values (water level measurements, gate positions, etc.): MITM (Man-in-the-Middle) attacks, etc.
    - Interference at the control level (actions on controllers, PLCs, remote, etc.) with the purpose of altering the normal functioning of the system: carrying out improper operations, unpredictable system operation, falsification of information received by operators, activation/inhibition of alarms, etc.
    - Interference with instrumentation (data manipulation to cause erroneous maneuvers).
    - Interference in the actuators in order to carry out improper operations or, alternatively, prevent manoeuvres (modification of configurations, start/stop orders for pumps, opening/closing of gates, etc.)

A detailed description of the most vulnerable threats is provided below, which can lead to important failure modes in a dam and other hydraulic facilities.

4.1 Access control failure.

4.1.1 Introduction

Access control is the set of devices to be implemented for the control, verification, identification, inspection, intervention or supervision of the passage or circulation of people, vehicles or objects to an area or enclosure previously defined as a control or security area for the prevention and protection against risks that may affect people, property and/or facilities [1].

Access control can be applied to people, vehicles, materials and objects. This control can also be autonomous or centralized and use physical, mechanical or electronic technical means, normally using a combination of the three.

The main access control systems are the following:

- Pedestrian access control: material credential, knowledge credential or personal credential
- Vehicle access control: license plate control, code verification, time and driver verification.
- Access control of materials and objects: explosives, weapons, explosive devices, others.

The health crisis caused by the COVID-19 pandemic has also introduced a new variable in access control, which is to prevent the spread of the epidemic. Based on this need, new tools have been introduced in access control, such as sensors to detect that personnel are entering with a mask or devices to control body temperature.

4.1.2 Failure modes

Access control fails when any unauthorized person, vehicle or object enters the premises, bypassing the access control system. This failure can be the gateway to threats of all kinds, potentially causing both physical and logical damage to the structure.

The following failure modes can be identified, among others, in access control:

- Undetected access failure.
- Failure due to unauthorized access through identity theft.

Access through the use of violent or expeditious methods can also be considered, although this is not a failure of the access control system as such, but rather the failure of passive security systems.

[1]Definition taken from the *"Manual for the Director of Security"*. Manuel Sánchez Gómez-Merelo. ET Technical Studies, SA. 1996.

Although it is not the subject of this section, it is worth emphasizing the need to complement the access control system with other installation protection systems such as:

- Physical protection systems for the perimeter and interior of the facilities.
- Remote surveillance systems.
- Coordination system with the corporate security centre and with the operational centres of the security forces and bodies.

4.2 Physical access cut.

4.2.1 Introduction

Cutting off physical access to the dam limits the organization's protection and self-protection actions.

Cutting off access is not in itself a risk element for the security of dams, but **in the case of sabotage it is a preliminary action to lengthen the reaction time** and provide the attacker with an additional period to undertake more far-reaching actions on the dam and its facilities.

4.2.2 Factors influencing cutting

Dams are located in places with very different access points. Some are located close to public roads and towns and have more or less frequent traffic. In such infrastructures, it is more difficult to carry out acts of sabotage.

However, many other dams are located in isolated places where the access road is a separate branch to the dam and there is little traffic, in these cases it is easier to cut off the access.

Access can be cut off by placing some element blocking the road (large rocks, trees, chains, etc.) or by destroying a section of it.

Among these actions, blocking is a relatively simple action to carry out since it does not require special means, and is therefore the one that should be considered the most likely.

Cutting off a section of road requires the use of larger equipment such as public works machinery or explosives and is therefore more complex to implement.

4.2.3 Regulations regarding access

The Technical Safety Standard for the design, construction and commissioning of dams and filling of reservoirs, approved by Royal Decree 264/2021 of April 13, indicates that: "*the dam and its facilities will be equipped with guaranteed access, even in adverse circumstances, unless specifically justified"* (art. 19.1).

The Technical Regulations for the Safety of Dams and Reservoirs (RTSPE) recommend that *the dam have alternative accesses to allow communication in extreme cases* (art. 22).

The Large Dam Instruction also indicates in a generic manner that access will be considered for the construction and maintenance of the dam (art. 23).

The Basic Guideline for Civil Protection against Flood Risk does not specify anything regarding access. However, when implementing Emergency Plans, it is common to enable several accesses to the dam and Emergency Room (main and alternative).

Although dams have different access points, it must be taken into account that the main access point is usually the most direct and the usual access route and that entry through the alternative access point, once the breach in the main access point has been discovered, will not be immediate. This must be taken into account when estimating reaction times in the event of sabotage.

4.2.4 Treatment in Emergency Plans

In dam emergency plans, access cuts have traditionally been classified as an indicator of "*difficulty of action* ", which is why specific procedures for dealing with them are not usually available. This is because the plans do not relate the cut to a subsequent attack. This fact should not be overlooked in the field of critical or strategic infrastructures and should be linked to the possibility of sabotage.

4.2.5 Assessing the severity of the cut

As indicated, the less traffic it supports and also the longer it lasts, the more vulnerable the access will be.

The consequences of the cut can be quantified based on the time that the dam will remain isolated. It will depend on the detection of the incident, the type of cut (blockage or destruction of the road) and the response time of the State Security Forces.

As for the detection of the incident, this may not take place until the obstacle is found on the road, so it is very likely that another action will be detected beforehand at the dam facilities. Therefore, the possibility of access being cut off must be reported to the State Security Forces as soon as the sabotage alarm is transmitted.

4.2.6 Other types of cutting

This section may also include power outages, telephone lines, data transmission lines and communications in general, which can leave the dam isolated and inoperative, especially those managed from centralized control centers. Cases related to interference in communications associated with remote supervision or operation are dealt with in the section **Error! Reference source not found.**dedicated to cybersecurity.

4.3 Drone attack.

4.3.1 Introduction

The drone, UAV (Unmanned Aerial Vehicle), or VANT (unmanned aerial vehicle), is an unmanned aerial vehicle capable of autonomously maintaining a controlled and sustained level of flight, and propelled by an internal combustion, electric or jet engine.

The concept of “unmanned” can lead to confusion, because, although there is no crew inside the vehicle, there is contact between the UAV and operators on the ground, and it can be linked to people on the ground, whether they are pilots, controllers or any other type of operator related to monitoring the aircraft. With this clarification, not everything that is in the air is considered a drone or UAV, since hot air balloons or missiles are not considered as such.

Drones can be controlled remotely from the ground by an operator, or they can be autonomous and follow a predefined trajectory or programmed flight plan. There are therefore two stations that can handle information from the drone, the ground station and the onboard station; depending on how autonomous the drone is, the ground station will perform more or less functions on a regular basis.

Its origins and subsequent development are due to the military needs that prevailed during the Second World War and the subsequent Cold War. A small plane capable of crossing enemy lines, gathering information and even reaching small targets without risking the life of any soldier. Subsequently, this military device has also become a useful tool for civil society, with the appearance of civil and commercial drones, used in all kinds of activities: surveillance of facilities, topography, geography, geology, agriculture, etc., and even for fighting fires or for rescue operations.

Drones are constantly advancing and innovating, improving their performance every day. Aside from military use, unmanned aerial vehicles are used in an increasing number of civilian applications, especially in tasks that are too "boring, dirty or dangerous" for manned aircraft.

Depending on the purpose for which it is designed, the UAV will have appropriate dimensions and technology to carry out the task at hand as best as possible. Because of this, drones come in a wide variety of shapes, sizes (from several meters in wingspan to a few centimeters), configurations and features...

The basic types of drones are as follows:

- According to the wings:

  - Fixed-wing drones: These have static wings and are similar to an airplane in their design and flight style.
  - Multirotor drones: They have several propellers that rotate in different directions, and can remain in the same place or change position.

- According to the control:

- Autonomous drone: does not need a pilot to control it, it is guided by its own systems and sensors.
- Remote controlled drone: The drone is piloted directly by a technician using a control device.
- Monitored drone: the drone directs its own flight plan, and the technician, although he cannot control the controls directly, can decide what action it will carry out.

- According to size:

- NANO-DRONE, Nano-UAV or NAV (Nano Air Vehicles): Nano-drones will be one of the future components of drone swarms.
- MICRO-DRONE, Micro-UAV, MAV or µUAV: Capable of being launched by hand and operating at ranges of up to 30 km, they generally have dimensions no greater than 15 cm.
- MINI-DRONE, mini-UAV or MUAV: These are UAVs weighing less than 25 or 30 kg, with ranges of over 30 km.
- Small Drones, Short-Range UAVs or Close-Range UAVs: Used in operations with a range of up to 100 km. The widest range of systems and vehicles can be found in this group.
- Tactical drones, TUAV- Medium Range, tactical UAV or Tactical UAV: Ranges between 100 and 300 km.
- MALE (Medium Altitude Long Endurance): Moderate operating altitude, between 5,000 and 15,000 meters, and high autonomy, up to 24 hours. Functions similar to the above. The operating range is usually lower (around 500 km).
- HALE (High Altitude Long Endurance): High altitude, over 15,000 meters, and over 24 hours of autonomy. Global reconnaissance and surveillance missions.
- And apart from that, the UCAV and UCAR, which are systems designed for combat weapons.

	Max. mass (kg)	Max. range (km)	Flight altitude (m)
ELDER BROTHER	< 0.5	5	50
MICRO	1.0	30	200
MINI	20	30	1000
LITTLE	150	100	8000
TACTICAL	1000	300	10000
MALE	8000	500	15000
HALE	20000	1000	25000

Table 1Classification of drones

The drones to be used against critical or strategic infrastructures could be of any of the types seen above, both those for military use (in the event of an armed conflict or organised terrorist groups) and those for civil use, which are usually smaller in size and with a load capacity (micro-drone, mini-drone and small drones).

However, this guide will not cover situations of armed conflict, so the following sections will refer only to civilian drones, which are more easily accessible to anyone who wants to use them against infrastructure.

4.3.2 Legislation considered

The drone sector has experienced significant growth in Spain in recent years, which is why there is a need to establish a new legal framework that allows for greater development in safe conditions in this technologically cutting-edge and emerging sector.

Royal Decrees 1036/2017 and 517/2024 have been approved, regulating drone operations, establishing the conditions that must be met by organizations designing, manufacturing and maintaining this type of aircraft, training requirements for piloting, measures relating to recreational, that is, non-professional use, establishing a series of limitations aimed at guaranteeing the safety of the airspace and the safety of citizens.

The Council of Ministers approved Royal Decree 1036/2017, of December 15, published in the BOE on Friday, December 29, 2017, regulating the civil use of remotely piloted aircraft, and amending Royal Decree 552/2014, of June 27, which develops the Air Regulations and common operational provisions for air navigation services and procedures and Royal Decree 57/2002, of January 18, which approves the Air Traffic Regulations.

Furthermore, the conditions now approved are supplemented by the general regime of Law 48/1960, of July 21, on Air Navigation, and establish the operating conditions with this type of aircraft, and other obligations.

The standard establishes requirements for operators to carry out activities using these devices safely in environments that were not previously permitted, such as buildings, open-air gatherings of people or night flights. The different scenarios and requirements in which specialized air operations, flights, sports, recreational, competition or exhibition activities may be carried out are contemplated.

The new regulation also allows operations to be carried out in controlled airspace, but this will require specific training and equipment requirements, as well as an aeronautical safety study coordinated with the air traffic service provider and prior authorization from the State Agency for Air Safety (AESA).

The document also sets out the conditions that organizations must meet for the design, manufacture and maintenance of aircraft, and indicates the training requirements for pilots, in line with the regulatory frameworks of other European countries.

Royal Decree 517/2024 regulates the use of UAS on critical infrastructures, establishing specific restrictions and conditions to protect these areas. In particular, it is mentioned

that the use of UAS in restricted areas that include critical infrastructures is subject to the prohibitions and restrictions established in previous regulations, such as Royal Decree 1180/2018. In this context, it is specified that:

- Environmental protection restricted areas and photographic flight restricted areas have specific regulations limiting the use of UAS in these areas.
- Critical infrastructures, which may include strategic and security facilities, are subject to stricter control to avoid risks to national security and the integrity of these facilities (Article 37 of the aforementioned RD 517/2024).

On citizen security:

Royal Decree 1036/2017 incorporates a series of complementary provisions given that the use of unmanned aircraft may affect public safety. In this regard, the law requires that the Ministry of the Interior be informed in advance of any operations with these devices that are carried out over urban areas and conurbations. It also reserves the authority of the authorities to limit the operation with drones for reasons of public safety.

RD1036/2017 develops the regulatory framework initially adopted by Royal Decree-Law 8/2014, which established minimum requirements for operations with this type of aircraft, but did not cover all the potential activities that the sector has subsequently raised.

Recreational use of drones:

This Royal Decree contains measures relating to the recreational use of drones, establishing a series of limitations aimed at guaranteeing the safety of the airspace and that of citizens. As a general rule, these flights must be carried out outside urban environments (unless the drone weighs less than 250 grams), during the day, more than eight kilometers from airports, always keeping the drone in sight at a maximum of 120 meters from the ground, in suitable weather conditions (no fog, no rain and no wind), in controlled airspace and without endangering people and property on the ground.

The requirements established in the Royal Decree are subject to the supervision and control of AESA and failure to comply with them constitutes an administrative offence in the field of civil aviation in accordance with the provisions of Law 21/2003, of July 7, on Air Safety.

4.3.3 Failure modes

Civilian drones do not, in themselves, pose a threat or danger. It is their use as a means of approaching an infrastructure carrying a dangerous element that poses a risk. These dangerous elements may be explosive or contaminating, the possible effects of which are discussed in the corresponding sections.

The malicious use of drones is a risk to be taken into account, for the following reasons:

- Civilian drones can be purchased in stores, online, and also in parts, and the prices are relatively affordable.
- They are easy to use for any user.

- They can transport up to 10-12 kg of any substance or element.
- They can be programmed to land at a specific location or to fly over a specific area.
- The largest ones can fly at speeds of up to 90 km/h.
- Flight autonomy depends on the batteries. From 20 minutes to 6 hours (drone with 6 batteries)
- They have GPS positioning. With this system, the degree of precision in the landing point and flight path is of the order of 2 to 5 m.
- With corrected GPS positioning, the degree of accuracy is centimeters.

4.3.4 References

- Royal Decree 1036/2017, of December 15, regulating the civil use of remote-controlled aircraft.
- Royal Decree 517/2024, of June 4, which develops the legal regime for the civil use of unmanned aircraft systems (UAS), and modifies various regulatory standards regarding the control of the importation of certain products with respect to the applicable standards regarding product safety; civil air demonstrations; firefighting and search and rescue and requirements regarding airworthiness and licenses for other aeronautical activities; registration of civil aircraft; electromagnetic compatibility of electrical and electronic equipment; Air regulations and common operational provisions for air navigation services and procedures; and notification of civil aviation events.
- Consolidated Implementing Regulation (EU) 2019/947 including changes to Implementing Regulation (EU) 2020/639 and Implementing Regulation (EU) 2020/746.
- Consolidated Delegated Regulation (EU) 2019/945 including changes from Delegated Regulation (EU) 2020/1058.

4.4 Sabotage by the organization's own personnel.

4.4.1 Introduction

When thinking about failure modes in a dam, possible sabotage by personnel from the organization itself is not one of the first that comes to mind. Perhaps this is because it is a world of highly specialized companies and, in general, tradition.

But it must also be taken into account that the organization's own personnel are the ones who know the installation best. This means that they have ease of movement and orientation inside the dam. Something that is not easy for someone who is not used to moving through galleries and installations of a dam. In fact, since each dam is unique, even for someone who is used to moving through this type of installation, it can be difficult and complicated to do so in an unknown dam. Therefore, the knowledge of the installation that the organization's own personnel has is a very valuable element in the event of attempting to carry out sabotage.

Someone in the organization who wants to cause harm may act on their own initiative (mental illness, spite towards their superiors or the company, bribery, etc.) or coerced by third parties who are interested in causing harm (e.g., kidnapping a family member, death threats, etc.).

In organisations with a large number of personnel involved in the operation of the dam, it is difficult for sabotage to be promoted individually. Therefore, to carry out sabotage that directly affects the civil works (e.g. blowing up parts of the dam) due to its magnitude, the complicity of a group of people from the organization involved would be required. This case is very unlikely in times of peace, although it should not be ruled out at any time.

It should be noted that contracting companies (contracted services) and their employees are also considered to be part of the organization's staff. This type of staff, as they do not belong directly to the organization, is more difficult to control, due to the lack of knowledge of the employees since the procedures they work with are specific to the contracting company.

Of interest is the reference indicated in the EU Directive CER 2557/2024 of upcoming transposition, on the possibility of consulting/checking the background of qualified personnel (article 14) who provide service in critical and/or vital assets of a critical/strategic infrastructure in accordance with the regulations and procedures established both at national and European Union level.

4.4.2 Failure modes

Once the most important aspects to take into account have been listed, let's look at the most representative possible Failure Modes related to sabotage by the organization's own personnel:

a. Improper operation of drainage organs
b. Power outage due to damage to dam equipment (transformers, generator sets, etc.)
c. Related to the above would be the illegal extraction and sale of copper electrical cables, which has been quite common in recent years.
d. If the term is allowed, one could also speak of a possible “indirect sabotage”, in reference to the intentional non-transmission of serious incidents/incidents that affect the safety of the dam.
e. Third-party attack facilitator.

4.5 Malicious activation of floodgates

4.5.1 Introduction

In general, a malicious gate actuation threat may result in one or more of the following mission losses, among others:

- Loss of flood control and smoothing function.
- Loss of water storage.
- Loss of hydroelectric production
- Cut in urban supply and irrigation.
- Loss of recreational use.

In addition, other events may be included, such as manipulation or breakage of other drainage organs, bottom drains, intakes, secondary infrastructures, etc., which also entail loss of mission or damage to the dam itself or downstream.

4.5.2 Failure modes

The following are possible failure modes that can result from malicious gate activation, including:

- OPENING OF THE SPILLWAY GATES.
- BLOCKING OF SPILLWAY GATES (INCEPTIBILITY OF OPENING).
- OPENING OF INTERMEDIATE DRAINS.
- BOTTOM DRAIN OPENING.
- OPENING OF SUPPLY INLETS.
- OPENING OF OTHER SHOTS.

4.6 Blasting or serious damage to dam elements.

4.6.1 Introduction

There is growing concern about the possible outcome of an explosive attack on a water infrastructure, a dam or its associated facilities. There are known plans to attack dams by terrorist or criminal groups, although the details, and in particular the degree of success, have not generally been disclosed.

Dam/Reservoir	Country	Plan frustrated	Organization	Description
Samarra	Iraq	2015	DAESH	500 kg of explosive
Salma	Afghanistan	2013	Taliban	1,300 kg of explosive
Falcom	US / Mexico		Zetas	Unknown
Chingaza	Colombia	2002	FARC	Unknown
Lhokseumawe	Indonesia	2001	Separatists	explosive device
Panauti Plant	Nepal	2001	Communist insurgents	explosive device
Kidapawan	Philippines	2003	Islamist insurgents	Rocket launcher
Kajaki	Afghanistan	2003	Islamist insurgents	Rocket launcher
Dumarao	Philippines	2004	Communist insurgents	explosive device
Selaghat	Nepal	2004	Communist-Maoist insurgents	explosive device
Mirani	Pakistan	2005	A stranger	explosive device
Haditha	Iraq	2005	A stranger	explosive device
Haditha	Iraq	2005	Islamist insurgents	Rocket launcher
Kajaki	Iraq	2005	Islamist insurgents	explosive device
Hlaingbwe	Myanmar	2007	Separatists	explosive device
Hlaingbwe	Myanmar	2007	Separatists	Grenade launcher
Waeng Station	Thailand	2007	Islamic separatists	explosive device
Kajaki	Afghanistan	2008	Islamic insurgents	explosive device
Tipaimukh	India	2008	A stranger	explosive device
Mosul	Iraq	2009	A stranger	explosive device
Balimela Power Station	India	2009	Communist-Maoist insurgents	incendiary device
Mytikyina	Myanmar	2010	Ethnic separatists	explosive device
Thawt Yin Kha	Myanmar	2010	Ethnic separatists	explosive device
Machlagho	Afghanistan	2011	A stranger	explosive device

Table 2Terrorist activities with explosives in dams.

Dam attacks carried out in war situations are also well known. The Geneva Conventions expressly prohibit (since 1977, with the amendment Protocol I) attacks on dams, but the

reality is that both before and after, such attacks have occurred. During World War II, the Allies, specifically the Royal Air Force of the United Kingdom, launched an attack on four German dams in the context of Operation Chastise. At the Mönhe and Eder dams, both gravity dams, the bombs managed to form a breach and empty the reservoir. On the other hand, at the Sörpe dam, made of loose materials, the bombs only managed to form a few craters in the downstream shoulder, without developing any failure mode that could compromise the stability of the dam. More recently, during the Balkan war, the Serbian army placed several tons of explosives in the gallery of the Peruca dam (in Croatia). The explosion produced a subsidence in the crown and craters in the abutments, but did not break the dam.

A terrorist attack is unlikely to be successful, but the existence of such threats is a cause for concern for dam owners and operators. Furthermore, even if they do not compromise the stability of the dam, attacks can affect its serviceability or harm people in the vicinity of the attack. It is therefore very important to determine what effect explosives can have on dams in the short and long term.

The problem of structural resistance to explosive loads has been the subject of research for many years, especially within the military community. Although much of this research is of limited use, there is also ample information available that may be useful to those engineers who design, build and operate such infrastructures.

In the case of buildings, Eurocode EN 1991-1-7 refers to accidental loads and explosions, but it focuses mainly on impulsive actions such as the impact of trucks, trains, ships, helicopters or any other vehicle in general. It also considers gas explosions in closed spaces, but there is no general framework for the treatment of external explosive loads. The CTE (Basic Document SE-AE Actions in buildings) only states that, in buildings with uses such as chemical factories, laboratories or warehouses of explosive materials, the specific accidental actions considered must be stated in the project, indicating their characteristic value and their model.

4.6.2 General information on explosives

Explosives are mixtures of chemical substances with a certain degree of instability in the atomic bonds of their molecules which, under certain circumstances or external impulses, lead to a rapid reaction of dissociation and regrouping of the atoms into more stable forms. This reaction, of the oxidation-reduction type, is known as detonation and produces gases at very high pressure and temperature, which in turn generate a compression wave that runs through the surrounding medium.

In this way, the chemical energy contained in the explosive is transformed into the mechanical energy of that compression wave, in a short space of time.

Based on chemical kinetics, a distinction is made between: **combustions** (chemical oxidation reactions in which a large amount of energy is generally released at a reaction speed of less than 1 m/s and which can be observed with the naked eye in the form of a flame), **deflagrations** (like combustions with flames, but developing at a speed lower

than the speed at which sound would propagate in the explosive itself and with pressure waves of the order of 10^3 atmospheres) and **detonations** (supersonic combustion - between 1,500 and 9,000 m/s - which generate a shock wave with high pressure gradients - 10^5 atmospheres - and temperature). The composition and characteristics of the explosive, among other variables, determine the detonation speed, as well as the bubble and detonation pressures.

4.6.3 Characteristics

The most relevant characteristics of an explosive are:

Explosive power	Capacity to break and project materials (effective blasting energy). It depends fundamentally on the composition.
Detonation velocity	The rate at which explosive material is transformed into gases. Slow-detonating explosives work better in softer materials and produce coarser fragmentation, while high-velocity explosives produce more intense fragmentation in harder materials.
Cartridge density	The higher the density of the explosive, the higher the charge concentration. It also depends on the composition and the manufacturing process. The relative density of explosives is normally between 0.8 and 1.5 (below 1.1 they do not work well submerged).
Water resistance	Ability to (in the absence of a special coating) maintain unaltered properties for a period of time in contact with water. Gelatinous dynamites, hydrogels and emulsions are perfectly resistant to contact with water, but powdery products and ANFOs are not (due to the soluble nature of ammonium nitrate). However, under certain conditions and in the form of an emulsion or saturated solution, it can offer good resistance to water. Virtually all types of explosives tolerate a certain amount of humidity, provided that the explosive remains in these conditions for a short time. In the case of bulk explosives such as ANFO, this resistance is due to the fact that they are sheathed and that additives are incorporated.
Sensitivity	Energy that must be transmitted (through a detonator, a shock wave, impact or friction) to cause its initiation and, subsequently, its detonation.

Table 3Characteristics of an explosive.

4.6.4 Classification of industrial explosives

According to the magnitude of the energy impulse necessary to initiate its detonation:

• *Primary explosive substances*: These are substances that, due to the weakness of their bonds, are highly sensitive and unstable. A small quantity of these substances is already sensitive to ignition (small critical mass). They are used in the manufacture of detonators. Examples: mercury fulminate, lead azide and lead trinitroresorcinate.

Acetone peroxide (triacetone triperoxide, peroxyacetone, "*mother of Satan* ", TATP) is a powerful primary explosive that has attracted the attention of terrorist groups because it

can be manufactured from household products. However, it is highly sensitive to temperature, friction and impact, making it difficult to handle.

• *Secondary explosive substances*: These are explosive substances whose detonation requires, in comparison with the previous ones, a greater quantity of explosive and a greater energy impulse. They are used as the base charge of detonators, as primers to initiate low-sensitivity explosives and also, to a greater or lesser extent, form part of the composition of many commercial explosives.

These substances include nitroglycerin, nitroglycol, trinitrotoluene, pentaerythritide and nitrocellulose.

• *Non-explosive substances that can be detonated* by a sufficiently high energy impulse (for example, the detonation of another explosive). Mainly ammonium nitrate (widely used in industry, as it is generally used as a fertilizer) which, by adding a combustible element that corrects its positive oxygen balance, forms part of most current commercial explosives. It is a practically inert product (which makes it very safe to handle) that is sensitized by adding around 5-6% by weight of diesel fuel and is very cheap. However, it is highly hygroscopic and soluble in water, which makes it desensitized to the point of making its detonation impossible. It has a heat of explosion of only 380 cal/g (approximately a quarter of that of nitroglycerin), but if a fuel is added it can be increased to over 900 cal/g.

Mixtures of these and other substances give rise to the most common industrial explosives, such as those shown below:

Industrial explosive	Composition	Characteristics
Powdered dynamite	Basically ammonium nitrate, a fuel and a quantity close to 10% of a sensitizer, which can be nitroglycerin, trinitrotoluene (TNT) or a mixture of both.	Low power Medium/low density (1.0 to 1.2) Regular or poor water resistance Detonation velocity of 2,000 to 4,000 m/s Little sensitivity to shock or friction. Rocks of medium-low hardness without the presence of water.
Gelatinous dynamite	Higher content of nitroglycerin (or Nitroglycol) plus a certain amount of nitrocellulose, which acts as a gelling agent, forming a gelatinous paste.	High power High density (from 1.4 to 1.5) Good or excellent water resistance. High detonation velocity (4,000 to 7,000 m/s) Some sensitivity to shock or friction. Recommended for high-resistance rocks, even in the presence of water.

ANFO	ANFO (Ammonium Nitrate + Fuel Oil), approximately 94% ammonium nitrate that acts as an oxidant and around 6% diesel oil that acts as fuel ALANFO (Aluminium + Ammonium Nitrate + Fuel Oil).	• Low/medium power. • Very low density (0.8). • Zero resistance to water, since ammonium nitrate is soluble and loses its ability to detonate. • Low detonation velocity (2,000 - 3,000 m/s). • They require another explosive (detonating cords, gelatinous dynamite primers, hydrogel cartridges or multipliers).
Hydrogels (slurries or explosive porridges)	An oxidising element (NH4NO3 or NaNO3) and another that acts as both a sensitiser and a fuel, and which can be an explosive (TNT), a metal (Al) or an organic salt (Monomethylamine Nitrate or Hexamine Nitrate) together with a certain quantity of water. A set of thickening, gelling and stabilising substances are usually also added to this mixture.	• High power. • Medium/high density (1.2-1.3) • Excellent water resistance • Detonation velocity of 3,500 to 4,500 m/s. • Less sensitivity to friction or impact. Great safety in handling and transportation.
Emulsions	A dispersed phase (small drops of NH4NO3 or NaNO3 solution in water) surrounded by a thin 10-4 mm film of mineral oil (continuous phase). That is, they are basically composed of ammonium nitrate or sodium nitrate with a water content of between 14 and 20%, approximately 4% diesel fuel and smaller quantities (1 – 2%) of other products, including emulsifying agents (sodium oleate or stearate), waxes to increase consistency and storage time, air or hollow glass spheres and aluminium particles that also increase their power and sensitivity.	All of this produces an explosive in the form of a paste, capable of being pumped or cartridged. • High detonation velocity (4,500-5,500 m/s) • Excellent water resistance. • Much less sensitivity to shock or friction.
ANFO mixtures with emulsion	From a 90/10 ratio, heavy ANFOs, to 50/50.	• Variable water resistance. • Densities between 1.25 and 1.10 g/cm ^{3}. • In cartridges or in bulk.

Table 4Classification of industrial explosives.

4.6.5 Conclusions

- Detonation produces an impulsive action (high pressures for intervals of the order of milliseconds).
- These detonations can have localized (crater and breccia formation) or general harmful effects.

- Different aspects of the explosive (material, quantity), the detonation point (distance and angle of exposure), the exposed material (concrete, earth, rubble) and the environmental conditions determine the importance of impulsive actions and localized breakages.
- Actions can in turn trigger different failure modes, although most do not seem viable due to the large amount of explosives required and the high degree of sophistication of the action they require.

4.6.6 References

- [Afriyie 2014] Effects of explosions on embankment dams, GA Afriyie, Master Thesis, Carleton University Ottawa, Ontario, 2014.
- [Bernaola Alonso et al. 2013] Bernaola Alonso, Jose; Castilla Gomez, Jorge and Herrera Herbert, Juan (2013). Drilling and blasting of rocks in mining. Polytechnic University of Madrid.
- [Busch 2016] Understanding the Behavior of Embankment Dams Under Blast Loading, CL Busch, PhD Thesis, University of New Mexico, 2016.
- [EUR 26456 EN] Calculation of Blast Loads for Application to Structural Components. JCR Technical reports, 26456 EN, European Commission
- [FEMA 2003] Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 427, 2003.
- [FEMA 2011] Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA-426, 2011.
- [FM 3-34.214] Explosives and Demolitions FM 3-34.214 (FM 5-250), Department of the Army – US, 2007.
- [Friedlander 1946] Friedlander, F. G. (1946). The diffraction of sound pulses. I. Diffraction by a semi-infinite plate. *Proceedings of the Royal Society of London A, 186*, 322–344.
- [Homeland Security 2012] Worldwide Attacks Against Dams, A Historical Threat Resource for Owners and Operators, 2012
- [IGME] Rock drilling and blasting manual. López Jimeno et al, IGME.
- [Jia 2016] Jia, JS, Xu, Y., Hao, JT and Zhang, LM, “Localizing and Quantifying Leakage through CFRDs”, Journal of Geotechnical and Geoenvironmental Engineering. Eng., 2016, 142(9).
- [Lampson 1946] Lampson, C.W., Explosions in Earth, Effects of Impact and Explosion, Office of Scientific Research and Development, 1946.
- [Nonveiller 1999] Nonveiller, E., J. Rupcic, and Z. Sever, "War Damages and Recon-struction of Peruca Dam", Journal of Geotechnical and Geoenvironmental Engineering, 125(4), 1999, 280-288.

4.7 internal and external drainage system.

The potential sabotage of the drainage system in masonry dams is analysed below, where both the dam body and the foundation constitute an essential element of the resistant mechanism. In general, masonry dams are considered to be those built using concrete and masonry, and among the resistant mechanisms, gravity dams are usually distinguished, which essentially mobilise friction in the contact between the dam and the foundation, in addition to mechanisms that incorporate an arch effect, with simple or double curvature. In all cases, masonry dams incorporate a drainage system that, on the one hand, limits the generation of underpressure forces in the foundation and, on the other, tries to keep the dam body free of flow.

4.7.1 Relationship between failure modes and drainage system sabotage

It is known that a failure mode is considered to be any situation or process existing in the dam-reservoir system that could cause the latter to stop providing the intended uses, and a failure mechanism is considered to be one of the potential sequences of events that may result in a failure mode. In this sense, sabotage or manipulation of the drainage system in factory-made dams does not constitute a failure mode in itself, but is actually an event that may form part of a failure mechanism.

In any case, sabotage of the drainage system is an event where malevolent anthropic action is concentrated, and which would be combined with the rest of the elements of the potential failure mechanism. If successful, the direct consequence of this event, which we could call "*sabotage of the drainage system"* , would therefore be the presence of flow lines and their corresponding hydraulic potential, with an increase in the pressures and associated underpressure forces, both in the foundation and in the body of the dam.

If historical statistics related to dam failures are analysed, subpressure forces always appear as one of the causes or fundamental elements of the failure mechanism.

In the case of the foundation, instabilities in which the existence of pressures that generate significant sub-pressure forces must be considered not only in the strict contact between the dam body and the foundation, but also in deeper planes or surfaces. On the other hand, there are differences depending on whether detachments can occur at the upstream foot, with the well-known formation of the tensile crack. Similarly, the conditions and nature of the rock mass can influence the mechanism due to the presence of more or less fractured material, and the very arrangement of the strata and families of joints can also result in different mechanisms, even mobilizing wedges of the ground, as happened in the failure of the Malpasset dam (ICOLD 2018).

Figure 14Left abutment of the Malpasset dam after failure, where a "dihedral" can be seen in the foundation with half of the gravity mass having collapsed. ICOLD TCDS, 2018

In the case of instabilities in the foundations of factory-made dams, the hydroelectric company BC Hydro developed an interesting summary of generic sliding or overturning mechanisms in 1995, differentiating the following:

1. Instability when the shear resistance is exceeded along a foundation discontinuity or in the vicinity of the dam-foundation contact, which could only occur in an extremely weak foundation, with faulty excavation or lack of foundation treatment.
2. Instability when a non-compressive area develops (tensile crack) and gives rise to an exceeding of the shear strength at the dam-foundation contact. This mechanism can develop in any type of foundation, even those of good quality.
3. Instability when the shear strength is exceeded along a pseudo-planar discontinuity of the foundation, which is also feasible in any foundation.
4. Instability when the shear strength is exceeded along a stepped discontinuity or one developed on several pseudo-parallel surfaces of the foundation. In this case, if the discontinuity surfaces are close together, the development of a failure envelope surface can be assumed, whereas, if the discontinuity surfaces are further apart, a more complex analysis will be required.
5. Instability due to exceeding the shear strength of a severely fractured or damaged foundation rock mass. This instability mechanism is rare, although it may be considered in the case of rock masses with multiple families of joints and fractures, where an enveloping planar fracture surface can be adjusted.
6. Instability when the shear resistance is exceeded along a combination of foundation discontinuities (not pseudo parallel as in the fourth mechanism). This type of mechanism can be initially simplified as type 3 or 4, although its analysis can be approached by limit equilibrium methods.
7. Instability due to buckling or overturning of pseudo-vertical strata in the foundation. This is an unlikely mechanism, but should be considered in highly

stratified and jointed rock masses with an almost vertical arrangement. This mechanism, if it exists, is usually combined with the second one.

8. Instability when the shear strength is exceeded on several three-dimensional surfaces of the foundation rock mass, forming an unstable dihedral or wedge due to the combination of faults, joints or fractures. This mechanism is unlikely, but it is precisely the one that developed in the aforementioned Malpasset dam, and logically requires a three-dimensional analysis.

For the dam body, the historic failure of the Bouzey dam empirically demonstrated the need for drainage, by means of the creation of perforations that draw the flow lines from the reservoir through the mineral skeleton of the concrete of the dams. This flow is usually concentrated at the ends of the dam blocks, where compaction of the concrete is more difficult and it is of poorer quality. The aforementioned perforations are empirically located close to the upstream face of the dam, separated from each other by about 3 m and connected vertically through the dam galleries, which are usually separated from each other by about 30-35 m.

Other classic references, such as the old "*Manual del vigilante de la presa* " (MOP, 1969), collect with different representations the role and importance of the drainage system, both in the body of the dam and the foundation, and the Spanish National Committee for Large Dams itself does so in several of its technical guides, such as those published with numbers 1, 2 and 6 (SPANCOLD, 2005, 2003, 1999).

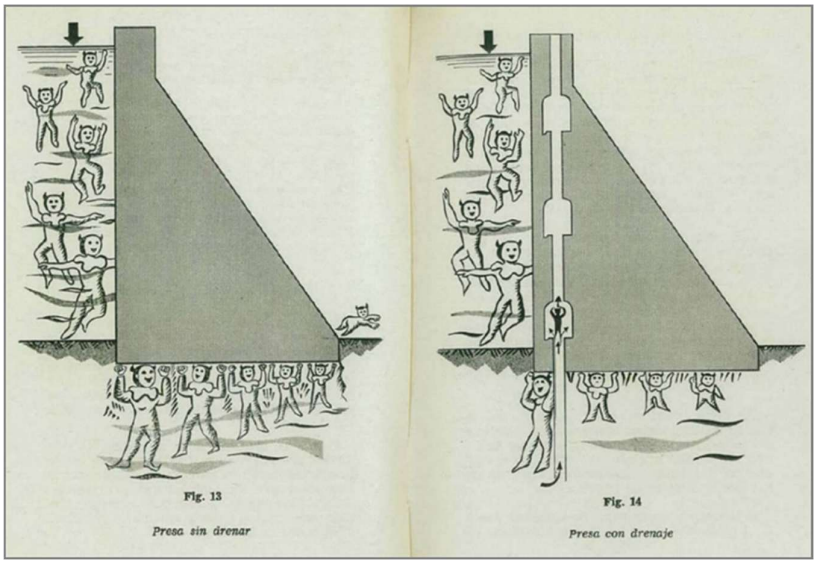

Figure 15Importance of drainage in gravity dams. Source: Dam watchman's manual. MOP, 1969.

Dam failures due to failures or problems with the drainage system at the foundation, which lead to a pathological increase in subpressures or destabilizing forces that develop at the contact surface between the dam and the foundation, or at the interfaces between strata or the joints of the foundation, constitute 17% of the historical cases collected by

several authors at the end of the last century. Currently (2020), the ICOLD is updating its database on dam incidents and failures, but in principle, it can be expected that this percentage will remain close to that figure, which implies one fifth of the failures.

Range	Description	No.	% of prey
Breakages			
1	Overturned	10	22
2	Underpressure	8	17
3	Leaks in the foundation	7	15
4	Internal erosion in the foundation	6	13
5	Excessive leaks	6	13
Accidents			
1	Leaks in the foundation	16	9
2	Local erosion/scour	16	9
3	Internal erosion in the foundation	13	7
4	Excessive leaks	13	7
5	Failure of drainage organs	10	6
Major repairs			
1	Freeze-thaw cycles	53	20
2	Extreme temperature gradients	28	11
3	Evolutionary reactions in concrete	22	8
4	Excessive permeability of concrete	22	8
5	Evolutionary reactions in masonry	22	8

Table 5Main causes of incidents or failures in masonry dams. Source: Douglas, Spannagle and Fell, 1998.

4.7.2 Conclusions on the sabotage of drainage systems

Based on the above information regarding sabotage of drainage systems in masonry dams, it can be established that malicious manipulation of the drainage system constitutes an event that could be part of the mechanism of several failure modes. In general, the potential failure modes of a dam can be developed in detail with the help of event trees or fault trees.

The main conclusion is that the chances of being able to cause a massive failure in a factory-made dam through malicious manipulation of the drainage system are very low.

Sabotage of the drainage system involves carrying out a series of tasks or actions that are complicated, even for someone who has knowledge of dam engineering or is familiar with them. On the other hand, these malicious actions would have a limited impact on the safety of the dam or its foundation, even if the necessary means were available to carry them out and, above all, the necessary time, given that these actions take a long time.

4.7.3 References

- Dam surveillance: Lessons learned from case histories – ICOLD Bulletin Draft. Technical Committee on Dam Surveillance, ICOLD, Paris, France, 2018.
- Manual on the use of explosives. Directorate General of Energy Policy and Mines, Spain, 2004.
- Technical Guide to Dam Safety No. 1. Dam safety. Spanish National Committee on Large Dams and College of Civil Engineers, Spain, 2005.
- Technical Safety Guide for Dams No. 2. Criteria for dam projects and their associated works (Volume I). Spanish National Committee for Large Dams and College of Civil Engineers, Spain, 2003.
- Technical Safety Guide for Dams No. 6. Construction of dams and quality control. Spanish National Committee on Large Dams and College of Civil Engineers, Spain, 1999.
- Manual of tunnels and underground works. ETSI Minas, UPM, Spain, 2000.
- Analysis of Concrete and Masonry Dam Incidents. UNICIV Report 373, University of New South Wales, Australia, 1998.
- Open Pit Blast Design. Julius Kruttschnitt Mineral Research Centre, The University of Queensland, Australia, 1996.
- Guidelines for the Assessment of Rock Foundations of Existing Concrete Gravity Dams, BC Hydro Report No. MEP67, Vancouver, British Columbia, Canada, 1995.
- Dam Watchman's Manual. Ministry of Public Works, General Directorate of Public Works, Spain, 1969.

4.8 Cybersecurity/cyber-physical risks.

4.8.1 Introduction.

A dam is an infrastructure that depends on a whole series of industrial and electromechanical equipment for its correct operation and exploitation. This equipment is integrated for its operation in control and supervision systems that include instrumentation, actuators, automatic controllers (PLC), remote units, supervisory terminals (HMI), etc. In addition, there is a whole series of systems that allow monitoring the state of the dam (monitoring systems), measurement and recording of hydrological parameters (flow rates, levels, etc.). These systems are increasingly integrated into local and remote communication networks, turning a dam into a cyber-physical system, which makes these infrastructures exposed to a series of threats that until very recently had not been considered. On the other hand, the way in which infrastructures are operated (maintenance, engineering, coordination between different actors, etc.) also introduces risks that must be managed.

We are currently facing a systemic risk scenario, in which a security incident in the physical realm can have implications for cybersecurity and vice versa, which makes a comprehensive approach necessary for the protection of these infrastructures.

In parallel to technical issues, there is also legislation that implies, in some cases, the need for the owners of the infrastructures to adopt a series of protection measures, such as the LPIC and the regulations that develop it. In accordance with what has already been said, these security measures must follow a comprehensive security approach, which includes cybersecurity. In those cases, in which an infrastructure has been included in the national catalogue of critical infrastructures (or which implies that its owner becomes, in turn, a critical infrastructure operator), the Operator Security Plan (PSO) and the Specific Protection Plans (PPE) are the basic security management tool. The provisions of Royal Decree-Law 12/2018, of September 7, on the security of networks and information systems and its regulatory development contained in Royal Decree 43/2021, of January 26, must also be taken into account in each infrastructure, if applicable in relation to operators of essential services.

It should be noted that industrial infrastructures, specifically their control and supervision systems (operational technologies or OT), have their own characteristics that differentiate them from corporate information systems (or IT technologies). For this reason, the direct transfer of security practices into IT systems must be avoided, as this may be ineffective or, in the worst case, affect the operation of the dam being protected. The participation of industrial cybersecurity experts is key in this matter.

It is important to note that the subsequent introduction of security measures on existing infrastructures often significantly affects their effectiveness and requires greater effort. For this reason, and as a general criterion, cybersecurity must be incorporated as an integral part of the project-construction-operation process.

4.8.2 Common weaknesses.

The CCN-CERT IA-04-16 guide [2]published by the National Cryptologic Centre contains a list of common weaknesses in organisations that manage infrastructures that depend on cyber-physical systems for their operation. All of them are applicable to large dams, and must therefore be analysed by those responsible for these infrastructures when defining the security strategy:

- Improper use of portable devices.
- Third party work.
- Inadequate management of interconnections with other networks.
- Poor backup management.
- Lack of staff awareness.
- Inadequate change management.
- Lack of adequate incident management and continuity plans.
- Poor information management.
- Poor software management.
- Poor assignment of responsibilities and safety management.
- Poor user and password management.
- Lack of technical management of security and systems.

Figure 16CCN_CERT Threat Report IA-04/16.

These weaknesses represent risk factors that may contribute to increasing the probability of a threat materializing or increasing its impact, and the organization must have technical, organizational and procedural controls aimed at eliminating or minimizing them. These aspects are discussed in detail in the following sections.

4.8.3 Assets.

The operation of a dam is supported by a set of assets consisting of structures and civil engineering elements, electromechanical equipment and instrumentation, control

[2]CCN-CERT, T. (2018). Risk Analysis in Industrial Control Systems (ICS). Report IA-04/16, Centro Criptologico Nacional, Madrid, 28 January 2016 (in Spanish).

systems, supervision and communication networks. To these, we must add other assets such as the personnel in charge of its operation and maintenance, whether owned by the dam or by third parties, and the information about it generated during the project-construction-operation process. Below is a list of assets that should be considered from a cybersecurity perspective:

- Accessible information about the systems themselves (supplier success stories, documentation associated with the project/construction/operation process, academic studies, websites of public or private organizations, etc.)
- Own or third-party personnel in charge of operation and maintenance.
- Remote interconnections for monitoring/maintenance.
- Integration interconnections in management systems (SAIH networks…)
- Instrumentation and actuators (level probes, flow meters, CCTV cameras, intrusion detectors, motor drives, valves or pumps, etc.
- Special purpose automated systems (monitoring, automatic alarm systems, etc.)
- Network and communications electronics (switches, routers, radio/3G/4G modems, serial/Ethernet gateways)
- Automation components (PLC, remote, local HMI).
- Remote or local monitoring systems (real-time servers, engineering stations, operating stations, time servers, etc.)
- Auxiliary equipment with remote management options (UPS, emergency generators, etc.)
- Security systems (monitoring, detection, alarm, etc.)

4.8.4 Failure modes.

In accordance with the above, cyber-physical systems are an integral part of a modern dam and can be used to alter its correct operation without having to resort to traditional physical methods such as those discussed in other points (see, for example, point 4.6on blasting or serious damage to elements of a dam). In addition, cybersecurity threats may be behind, in whole or in part, the risk scenarios already analysed, such as malicious activation of floodgates, sabotage, etc.

The operation of a dam can be altered both actively (for example, by directly operating the gates) and passively (by preventing them from being operated when necessary) or even by causing improper operation through action or omission by those responsible for the infrastructure by falsifying the information received at remote monitoring stations.

Following the classification included in the document *The Industrial Control System Cyber Kill Chain* published by SANS-ICS, [3]the actions of an attacker can be classified as follows:

- Loss of vision.
- Loss of control.
- Denial of view.
- Denial of control.
- Denial of safety.
- Manipulation of View.
- Manipulation of Control.
- Manipulation of Sensors and Instruments.
- Manipulation of Safety.

To interpret the situations described above, the following must be taken into account:

- *Denial* is the condition in which the system operator is temporarily denied access or the ability to perform an action. This does not necessarily have to immediately result in an impact on the operation of the infrastructure, as this depends on the length of time this condition is maintained, the context in which it occurs, etc.
- *Loss* is the condition in which the ability to monitor the state of a system (view) or effective control of it (control) is lost. Unlike denial, it will remain even after the attacker's interference has been removed.
- *Manipulation* is the condition by which an attacker carries out actions directly against a system in order to alter its mode of operation, which immediately results in a modification in the operating conditions of the infrastructure.

The application of each of them to an asset defines the failure modes. It should be noted that the same result can be produced by a deliberate action or by a random action (undirected malware or an accidental error in operation).

From a specific cybersecurity perspective, and with a focus on cyber-physical systems, the threats considered are the following:

- Interference in monitoring software.
- Interference in network and communications electronics.
- Interference in communications.
- Interference at the control level.
- Interference with instrumentation.
- Interference in the actuators.

[3] Assante, M.J., & Lee, R.M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room , 1* .

Below is a set of tables that relate the existing threats to a dam's cyber-physical systems, their application to the assets set out above, and some examples of the potential associated impact.

THREAT	AFFECTED SYSTEM	MECHANISM	OBJECTIVE (SANS ICS)	POSSIBLE IMPACT	EXAMPLE
Interference with monitoring software	Local or centralized SCADA system	Encryption (ransomware) of real-time servers, HMI.	Loss of view Denial of control	Inability to view or act on the status of the remote system.	Inability to view the current status (levels, capacities, gate positions) or act through the system's HMI interfaces.
	Local or centralized SCADA system	Unauthorized access to monitoring or management interfaces.	Loss of safety Denial of view Denial of control	Carrying out improper operations.	Opening or closing of gates. Elimination of legitimate users. Configuration changes, deployments, etc.
	Local or centralized SCADA system	Unauthorized access to software.	Denial of view Loss of view Denial of control Loss of control View manipulation	Carrying out improper operations. Unpredictable system operation. Falsification of information received by operators.	Using the system to access other remote infrastructures.

Table 6Existing threats to the cyber-physical systems of a dam. Interference with monitoring software

THREAT	AFFECTED SYSTEM	MECHANISM	OBJECTIVE (SANS ICS)	POSSIBLE IMPACT	EXAMPLE
Interference in network electronics and communications	Switches, serial/Ethernet gateways, routers, modem (3G/4G/radio) etc.	Modifying network settings.	Denial of view Loss of view Denial of control Loss of control	Inability to view or act on the status of the remote system. Unpredictable system	Inability to view the current status (levels, capacities, gate positions) or act through the

				operation due to loss of communications between its components (instrumentation, actuators, controllers, remote stations, etc.)	system's HMI interfaces or even in local mode.
Interference in communications	Communication networks	MitM	View manipulation Loss of safety	Falsification of information received by operators. Carrying out improper operations by operators.	Representation of false values (water level, gate position, etc.)

Table 7Existing threats to the cyber-physical systems of a dam. Interference in network electronics and communications.

THREAT	AFFECTED SYSTEM	MECHANISM	OBJECTIVE (SANS ICS)	POSSIBLE IMPACT	EXAMPLE
Interference at control level	PLC, remote, etc.	Writing records to PLC/remote memory	Loss of control Loss of safety View manipulation Manipulation of control	Carrying out improper operations. Unpredictable system operation. Falsification of information received by operators. Alarm activation/inhibition.	Opening or closing of gates.
	PLC, remote, etc.	Stop command	Loss of control Loss of safety Loss of view	Unpredictable system operation.	PLC stop that stops automatic regulation and the ability to remotely operate/display certain variables.
	PLC, remote, etc.	Manipulation of settings, program, etc.	Loss of control Loss of safety Loss of view	Unpredictable system operation.	Modification of the program in a PLC so that it

			Manipulation of control	Carrying out improper operations.	functions in a way not intended.

Table 8Existing threats to the cyber-physical systems of a dam. Interferences at the control level.

THREAT	AFFECTED SYSTEM	MECHANISM	OBJECTIVE (SANS ICS)	POSSIBLE IMPACT	EXAMPLE
Interference in instrumentation	Sensors, probes, IP cameras, general instrumentation	Changing settings/calibration	Loss of control Loss of safety Loss of view Manipulation of sensors and instruments	Unpredictable system operation. Carrying out improper operations by operators. Falsification of information received by operators. Alarm activation/inhibition. Loss of image supervision.	Carrying out incorrect measurements leads operators to take inappropriate actions.

Table 9Existing threats to the cyber-physical systems of a dam. Interference in instrumentation.

THREAT	AFFECTED SYSTEM	MECHANISM	OBJECTIVE (SANS ICS)	POSSIBLE IMPACT	EXAMPLE
Interference in actuators	Starters, frequency converters, pumps, UPS, motorized or pneumatic valve actuators and other types of equipment.	Modifying the settings	Loss of control Loss of safety Loss of view Denial of control	Unpredictable system operation. Inability to act on the remote system.	Changing the communication options settings of a static starter, which may prevent a motor or pump from operating.

	Starters, frequency converters, motorized or pneumatic valve actuators, UPS, generator sets, other types of equipment.	Writing logs to device memory	Loss of safety	Carrying out improper operations.	Shutdown of a UPS, leaving the equipment powered by it without power supply.

Table 10Existing threats to cyber-physical systems of a dam. Interferences in actuators

4.8.5 References.

- Assante, M.J., & Lee, R.M. (2015). The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room, 1.

- CCN-CERT, T. (2018). Risk Analysis in Industrial Control Systems (ICS). Report IA-04/16, Centro Criptologico Nacional, Madrid, 28 January 2016 (in Spanish).

- Directive 2022/2555 of the European Parliament and of the Council, known as **NIS2**, is the cybersecurity legislation adopted for the entire European Union

4.9 Intentional contamination of reservoir water.

4.9.1 Introduction

Any act of sabotage seeks to violently influence the opinion of a third party in order to achieve certain objectives. Thus, the purpose of an act of sabotage may not only be to cause victims or economic and environmental damage, but also to discredit the organization or demonstrate to society how vulnerable it can be.

In the field of water pollution, the same rules apply. It would not only be a matter of introducing substances into the water that could cause serious harm to people, but also of forcing us to breach some of the parameters that we have imposed on ourselves as a society to preserve our health and the environment in the long term. Sometimes it might even be enough to add harmless tracers or dyes to cause alarm and concern, or to circulate rumors and lies in the media or social networks to misinform and discredit the institutions or companies that manage it.

4.9.2 Failure modes

The failure mode is the contamination of water in the different phases of its storage or distribution, with the intention of causing damage or discredit to health, the economy, institutions, the environment, generating social alarm, creating media notoriety, etc.

The storage and distribution of water supply has several phases (high and low) with different behavior.

There are numerous cases of attacks related to water infrastructure, which have been described in section 3: “Historical Cases”.

Fortunately, there are no known major cases of water contamination in Spain.

The threat of contamination in the surroundings of a reservoir has a low probability of occurrence, only the case of Denmark (2006) is known, and due to the large volumes necessary for its contamination and the long residence times, it greatly limits the damage to human health. Although it is unlikely, it is possible and we must be prepared to face it.

4.9.3 Legislation considered

Two regulations have been considered that establish the mandatory quality criteria for water intended for human consumption and those intended for the environmental quality of water bodies.

Of the two, the most restrictive is the one aimed at the environmental quality of surface waters because it is more recent in its publication.

- Royal Decree 817/2015, of September 11, establishing the criteria for monitoring and evaluating the state of surface waters and environmental quality standards

- Royal Decree 140/2003, of February 7, establishing the health criteria for the quality of water for human consumption

4.9.4 Toxic products potentially used to contaminate water

There are a large number of compounds that could be deployed by terrorists or malicious people in an attack on the water supply and which are internationally referred to by their initials, such as Nuclear, Biological, Chemical and Radiological (NBC-R):

- **Chemical compounds used in water treatment:** These compounds, such as chlorine or fluoride, which improve water quality in the right doses, can become toxic in excessive quantities. These chemicals are very easy to obtain, since they are already inside the facilities, and improper handling, whether intentional or accidental, can have serious consequences. In addition, in automated systems, they can be the target of cyberattacks and cause damage from thousands of kilometers away.
- **Heavy metals:** Heavy metals are dangerous agents due to their toxicity to humans (mercury, cadmium, lead, nickel, etc.). They are also fairly easy to obtain, and their salts are usually easily soluble.
- **Herbicides:** As a general class, herbicides tend to be less harmful to humans than some other compounds, although there are some notable exceptions. However, they are very easy to obtain in large quantities, to distribute, and their presence goes unnoticed in the rural world, which increases their possible use in reservoirs, ponds, canals, etc. Although they would not cause many deaths, the panic caused by their presence in distribution networks could be serious.
- **Insecticides:** These tend to be more harmful to human health than herbicides. Some insecticides have chemical structures very similar to some of the chemical warfare agents. Like herbicides, insecticides are also available in large quantities and are easy to distribute. In some cases, their solubility limits their usefulness as weapons introduced into water, but others are very soluble and pose a clear threat.
- **Nematocides and Rodenticides:** Nematocides (pesticides from tiny worm-like animals) are similar to insecticides. With a few exceptions, they tend to be more soluble than insecticides. Some nematocidal compounds are also similar to chemical warfare agents in their structure and mode of action. Rodenticides (pesticides used to kill rodents) are of concern because they are specifically designed to be lethal to mammalian species such as humans. Both classes are available in large quantities.
- **chemicals and miscellaneous agents:** There are a myriad of industrial chemicals that could be used in an attack. The main one is cyanide, which is widely used in mining and other industries.
- **Radionuclides:** The use of radionuclides as weapons is a distinct possibility. Even if casualties are low, the psychological impact of a radiological threat could be severe. High-purity compounds, highly radioactive material, such as plutonium or uranium-238, are difficult and expensive to obtain, and a terrorist organization

that has obtained these materials is unlikely to be willing to use them in an attack on a supply system. The most likely outcome is low-level radioactive materials or waste.

- **Agents of war:** agents of chemical warfare such as VX, Soman, Sarin or Mustard Gas. It is unlikely that it was used against the water supply system because its aerosol effects are much more devastating.
- **Toxins and Bioagents:** There are a number of protozoa, bacteria, viruses and toxins that could be used in an attack. Many of these materials are extremely toxic, with compounds such as botulinum toxin being some of the most toxic substances known. These types of materials are fairly easy to obtain, there are several examples of ricin being produced by terrorists for these purposes (England, 2010). Bacteria can also be easily cultured, in fact even sewage could be used as a potential contaminant for a backflow attack.

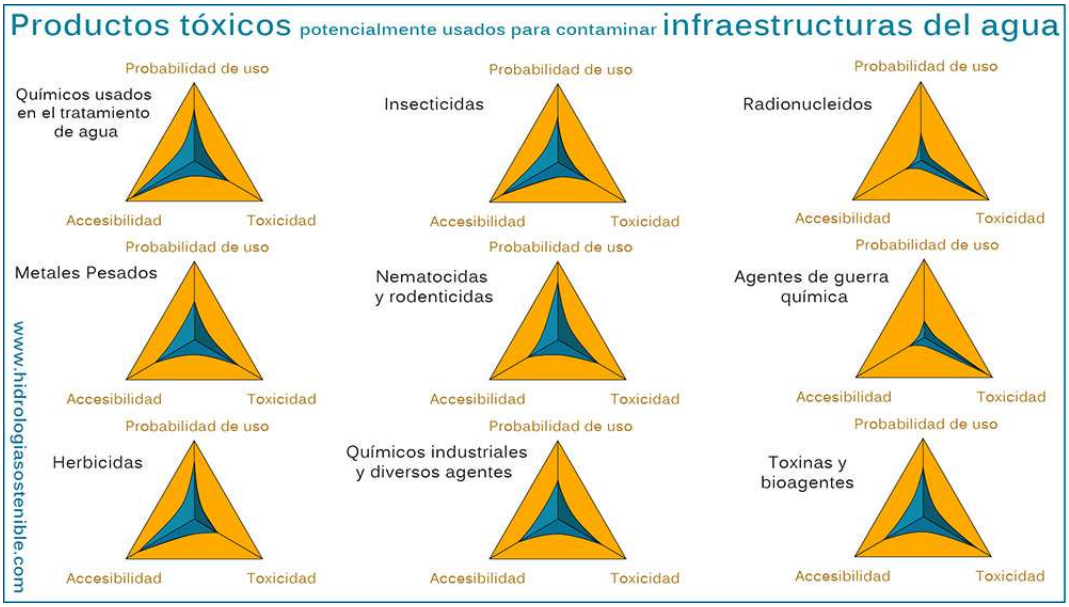

Illustration 17Toxic products potentially used to contaminate water infrastructure.

4.9.5 Conclusions of intentional water pollution.

The probability of malicious contamination of a reservoir with toxic substances is very low, as evidenced by the few cases recorded (one case in Denmark, 2006). It is even more unlikely that this contamination of the reservoir would cause harm to humans, since there is a large volume of dilution and a very long response time. However, it is a possible risk and therefore we must be prepared to face it.

5 RISK ANALYSIS.

Law 8/2011, which establishes measures for the protection of critical infrastructures, in its article 2, defines "*risk analysis* " as *the study of the hypotheses of possible threats, necessary to determine and evaluate the existing vulnerabilities in the different strategic sectors and the possible repercussions of the disruption or destruction of the infrastructures that support them* .

5.1 Methodology to be used

In order to identify and manage the main risks to which critical assets of an infrastructure are exposed, it is necessary to use one or more methodology, considering security in a global way, and analyzing the threats, both physical and logical, that may affect each of the assets.

Although there are many methodologies, perhaps the most widely used internationally for risk analysis are SEPTRI, MOSLER and MAGERIT.

The SEPTRI methodology assesses consequences in economic terms and its scope of application is not restricted to a specific hazard, but is suitable for assessing any hazard factor.

The MOSLER methodology is considered a quantitative method, although risk classification is considered a qualitative phase of the same.

The MAGERIT methodology is directly related to the generalization of the use of information technologies, and was developed by the Higher Council of Electronic Administration.

It should be noted that the SEPTRI and MOSLER methodologies are fully compatible and complementary, so they can be used together. For example, it is common to use SEPTRI/MOSLER methodologies for the physical part and MAGERIT for the cybersecurity part in corporate or purely IT systems, without forgetting the need to integrate the three methodologies based on the terms of probability and impact as a result of the risk. In addition, there are specific methodologies for carrying out risk analyses of industrial equipment and systems, such as the one described in the IEC 62443 standard (part 3-2).

5.2 Vulnerability Index.

Whatever the methodology used, the first thing that must be considered is determining the Vulnerability of each of the infrastructure assets.

For its determination, this Guide uses the documentation of the BIA2010-17852 project "Incorporation of Anthropic Risk components into the integrated safety management

systems of dams and reservoirs", developed in the period 2011-2013 at the Polytechnic University of Valencia (UPV), financed by the Ministry of Science and Innovation within the framework of the National R&D&I Plan 2008-2012.

The following table summarizes the levels of anthropogenic risk analysis that can be considered and their characteristics.

Level	Guy	Object	Use of risk models	Probability of failure	Consequences	System vulnerability	Risk results	Take of decisions
Essential	Qualitative Quantitative	Preliminary analysis	No	No	Basic to Intermediate	Essential	No	Screening Identification of the need for detailed studies.
Intermediate	Qualitative Quantitative	Global analysis of the dam portfolio	Natural threats	Probability of failure due to natural hazards (hydrological scenario)	Intermediate	Basic to Intermediate	Risk in hydrological scenario Anthropic risk conditional	System management Analysis of risk reduction measures
Advanced	Quantitative	Detailed analysis at a global (portfolio) and individual (prey) level	Natural threats and anthropogenic threats	Yes	Intermediate to Advanced	Intermediate to Advanced	Yes	Comprehensive system management Optimization and prioritization of risk reduction measures

Table 11Levels of analysis of anthropogenic risk in dams. Source: Project BIA2010-17852.

For the **basic level**, a global index of consequences for attack scenarios identified for the system is proposed, which is presented in the following table:

Descriptor Category	Very high Score = 10	High Score = 8	Half Score = 6	Low Score = 4	Very low Score = 2
Society	Population at risk (PAR): PAR > 1,000	Population at risk: (PAR = 100-1,000)	Population at risk: (PAR = 10-100)	Population at risk: (PAR = 1 - 10)	There is no population at risk
Economy	Disruption of essential services at national or multiregional level (>1,000 M€)	Disruption of essential services on a multi-regional scale (100 - 1,000 M€)	Disruption of essential services on a regional scale (10 - 100 M€)	Disruption of essential services at local or regional level (< 10 M€)	There is no interruption of essential services Local damage
Environment	Very serious or irreparable environmental damage	Serious or difficult-to-recover environmental damage	Severe to moderate environmental damage and 1 to 2 years of recovery	Moderate environmental damage (<1 year recovery)	Minor environmental damage

Table 12Example of estimation of consequences at a qualitative level (DAMSE, 2008).

In addition, a global vulnerability index is included as a preliminary analysis in dam-reservoir systems for anthropogenic risk that depends on the following factors:

- ACCESSIBILITY
    - Accessibility to the crest and body of the dam: by road, secondary road, private road, barriers.

  - Accessibility to the spillway / Drainage Organ (OD): from barrier-free road to closed perimeter.

- CONTROL OF SPILLWAYS/DRAINAGE ORGANS
  - Accessibility to control controls: barriers, accessible area.
  - Control operation: activated, possible activation or disconnected.
- SECURITY and DETECTION
  - Security systems: cameras, sensors and alarms
  - Dam staff: Permanent/regular/occasional presence of staff at the dam.
  - Frequent/daily, weekly or occasional inspection.
- COMMUNICATION:
  - Multiple communication channels, independent supply, failures, coverage.
- ANSWER:
  - Security forces: surveillance and visits by security forces, access, frequency and communication with staff.

These factors, grouped into five categories, are analyzed based on the information available in the documentation for each dam and, fundamentally, on the data collected during field visits. Each of the factors described above is evaluated using the descriptors in Table 17 and assigning the weights defined in Table 16.

Category	Subcategory	Weight (w)
ACCESSIBILITY	Prey	10
	Spillways and drainage organs	15
OD CONTROL	Access controls	10
	Activating controls	5
SECURITY/ DETECTION	General	20
	Dam staff	10
	Incident detection	10
COMMUNICATION	Indoor/outdoor communication	10
ANSWER	Security forces	10
Total		100

Table 13Weights established for the calculation categories of the global vulnerability index. Source: BIA2010-17852 Project.

Therefore, the global vulnerability index is obtained from the following expression:

$$IGV = \frac{\sum_{i=1}^{n} w_i d_i}{\sum_{i=1}^{n} w_i}$$

where *i* indicates the subcategory considered (out of a total of n=9 subcategories), w_i is the weight of each subcategory and d_i is the numerical value corresponding to the assigned descriptor.

A low index indicates a dam with low accessibility, greater possibility of incident detection, better communications, a high level of surveillance, etc. The maximum value of the global vulnerability index is equal to 5.

This index characterizes the general vulnerability of the dam to anthropogenic threats (it does not consider the vulnerability of each element separately, nor the potential consequences).

Below is a table with guidelines for assigning values for each subcategory based on the characteristics of the dam.

Category	Subcategory	Proposed values of the system vulnerability descriptor (d)
ACCESSIBILITY	ACCESSIBILITY (I) Accessibility to the crown and body of the dam	5: by road 1: private road/barriers
	ACCESSIBILITY (II) Spillway Accessibility / OD	5: from the road, without barriers 1: closed perimeter
OD CONTROL	ACCESSIBILITY (III) Accessibility to control knobs	1: several barriers 5: accessible area, without barriers
	CONTROL OPERATION	5: current 3: Disconnected, but activation possible 1:disconnected
SECURITY/ DETECTION	SECURITY SYSTEMS	5: There are no security/surveillance systems 3: Cameras 2: Cameras and alarms 1: Cameras, motion sensors.
	INCIDENT DETECTION	5: Unusual inspection 3: Weekly 1: Daily inspection
	PRESENCE OF STAFF Presence of personnel at the dam	5: Remote location 2: daily, but there is no town 1: staff resides in the vicinity of the dam
COMMUNICATION	COMMUNICATION Communication systems	5: failures, no coverage 1: Multiple paths, independent operation
ANSWER	SECURITY FORCES Surveillance Security Forces	5: Very Low (no communication protocols, no visits) 3: Medium (unusual visit, but keys and access) 1: Very High (frequent visits, communication)

Table 14Table estimating the vulnerability of the system at a qualitative level.

From these indices assigned to each category, a global index is obtained that identifies the vulnerability of the dam-reservoir system, as shown in the following table.

Descriptor (referring to system vulnerability)	Assigned value (d)
Very High	5
High	4
Average	3
Moderate	2
Low	1

Table 15Descriptors used to calculate the global vulnerability index.

5.3 Analysis of each Asset

Below is a description of the main elements of the risk analysis of a hydraulic regulation work. Each threat requires a specific analysis and the values assigned in the following table to the risk levels are only general recommendations (only for the full version):

RISK ANALYSIS		
Asset	Dimension	Threat
Dammed water	Physics	Mass poisoning
Dam body + galleries	Physics	Explosives in suicidal people
		Explosives in manned ground vehicles (suicides)
		Explosives in unmanned ground vehicles
		Explosives in unmanned aircraft
		Explosives in boats or manned boats
		Explosives in boats or unmanned vessels
		Explosives in stopped vehicles
		Explosives placed or abandoned
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Theft
Waterproofing screen	Physics	Explosives in unmanned aircraft
		Explosives placed or abandoned
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Vandalism
Drainage System in Galleries	Physics	Explosives in suicidal people
		Explosives placed or abandoned

		Armed terrorist attack
		Illegal Occupation
Spillways	Physics	Explosives in suicidal people
		Explosives in unmanned ground vehicles
		Explosives in boats or manned boats
		Explosives in stopped vehicles
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Sabotage
		Theft
Bottom drain	Physics	Explosives in suicidal people
		Explosives in manned ground vehicles (suicides)
		Explosives in unmanned ground vehicles
		Explosives in unmanned aircraft
		Explosives in stopped vehicles
		Explosives placed or abandoned
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Sabotage
		Theft
Take	Physics	Explosives in suicidal people

		Explosives in manned ground vehicles (suicides)
		Explosives in unmanned ground vehicles
		Explosives in unmanned aircraft
		Explosives in stopped vehicles
		Explosives placed or abandoned
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Sabotage
		Theft
Emergency Room Building / Technical Archive	Physics	Explosives in suicidal people
		Explosives in manned ground vehicles (suicides)
		Explosives in unmanned ground vehicles
		Explosives in unmanned aircraft
		Explosives in stopped vehicles
		Explosives in packages sent by mail
		Explosives placed or abandoned
		Grenade launcher/mortar attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Sabotage
		Theft

Administrative or control building	Physics	Explosives in suicidal people
		Explosives in manned ground vehicles (suicides)
		Explosives in unmanned ground vehicles
		Explosives in unmanned aircraft
		Explosives in stopped vehicles
		Explosives in packages sent by mail
		Explosives placed or abandoned
		Grenade/mortar launcher attacks
		Armed terrorist attack
		Arson
		Bomb Threat
		Heist
		Vandalism
		Illegal Occupation
		Sabotage
		Theft
Dam staff	Confidentiality	Assault and extortion
		Social engineering
	Physics	Assault and extortion
		Social engineering
	Availability	Assault and extortion
		Social engineering

Table 16Main elements of the risk analysis of a hydraulic regulation work.

The following tables contain the most significant potential threats identified:

Risk Code: RF.01	Threat: Mass Poisoning
Description: A malicious actor or organization discharges water into the reservoir in order to contaminate or poison the water so that it cannot be used for consumption and/or irrigation.	

Risk Code: RF.02	Threat: Damage caused by explosives carried by people
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.03	Threat: Damage caused by armed terrorist
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.04	Threat: Damage caused by bomb threat
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.05	Threat: Damage caused by explosives in land vehicles
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.06	Threat: Damage caused by explosives to boats or launches
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.07	Threat: Damage caused by explosives in aircraft
Description: A malicious actor or organization attacks physical elements of the dam with explosives in order to disable it or cause serious accidents downstream with repercussions on the affected population.	

Risk Code: RF.08	Threat: Assault and extortion

Description: A malicious actor or organization acts on a company employee with the aim of committing or collaborating in the commission of criminal acts that affect the essential service that the company provides to the population. The action on the employee may be aggressive, coercive or psychological.

Risk Code: RF.09	Threat: Intentional unavailability of staff
Description: A malicious actor or organization acts on a company employee with the aim of committing or collaborating in the commission of criminal acts that affect the essential service that the company provides to the population. The action on the employee may be aggressive, coercive or psychological.	

Risk Code: RF.10	Threat: Social engineering
Description: A malicious actor or organization acts on a company employee with the aim of committing or collaborating in the commission of criminal acts that affect the essential service that the company provides to the population. The action on the employee may be aggressive, coercive or psychological.	

Risk Code: RF.11	Threat: Common crime
Description: A malicious actor or organization (not of a terrorist nature) illegally accesses the dam's premises to carry out theft or robbery for primarily lucrative purposes.	

Risk Code: RF.12	Threat: Unlawful occupation
Description: A malicious actor or organization (not of a terrorist nature) illegally accesses the dam's facilities with the aim of occupying a facility, preventing its correct management.	

Risk Code: RF.13	Threat: Damage caused by the general public
Description: Actions produced by vandalism	

Risk Code: RF.14	Threat: Damage caused by sabotage
Description: Actions produced by criminals or the general public without profit motive that may affect the normal operation of the dam	

Risk Code: RF.15	Threat: Damage caused by arson

Description: Actions produced by criminals or the general public without profit motive that may affect the normal operation of the dam

Risk Code: RT.01	Threat: Access to technical documentation of the dam
Description: Unauthorized access to technical documentation of the dam available on local or remote computer systems. This could facilitate an attack by a criminal.	

Risk Code: RT.02	Threat: Interference with monitoring software.
Description: Actions performed on the supervision software (SCADA interfaces, HMI, etc.) that prevent remote or local operations from being carried out, the recognition of the current state of the system or that show a fictitious state that causes improper maneuvers to be carried out.	

Risk Code: RT.03	Threat: Interference in network electronics and communications.
Description: Actions carried out on the configuration or availability of communications equipment (routers, firewalls, switches, gateways, etc.) that prevent the correct functioning of the system, either by preventing the normal functioning of the communications networks or by preventing remote access to these devices.	

Risk Code: RT.04	Threat: Interference in communications.
Description: Actions performed on communications, for example interception or modification of transmitted information.	

Risk Code: RT.05	Threat: Interference at the level of control.
Description: Actions performed on equipment at the control level (PLC, controllers, etc.) that result in unintended operation of the automatic regulation systems.	

Risk Code: RT.06	Threat: Interference with instrumentation.
Description: Actions performed on the instrumentation (flow meters, level meters, pressure meters, position indicators, etc.) that affect its normal operation, causing unforeseen operation or the performance of improper maneuvers (modification in calibration, for example).	

Risk Code: RT.07	Threat: Interference in actuators.
Description: Actions performed on the actuators (opening/closing gates, for example) that result in unexpected or catastrophic results.	

Table 17Most significant threats detected.

6 MEASURES.

According to the Resolutions of November 15 and 29, 2011, of the Secretary of State for Security of Spain, on "*Minimum Contents of the Specific Protection Plan* ", there are three types of measures:

6.1 Organizational or management measures

The Operator must indicate whether it has at least the following organizational or management measures in place, and the scope of each of them:

- Risk Analysis: Evaluation and assessment of threats, impacts and probabilities to obtain a risk level.
- Definition of roles and responsibilities: Assignment of security responsibilities.
- Defined regulatory body: security policies, procedures and standards
- Rules and/or regulations applicable to strategic or critical infrastructure, as well as identification of their level of compliance.
- Certification, accreditation and security evaluation obtained for critical or strategic infrastructure.
- Certification of "safe space" in a health epidemic situation.

6.2 Operational or procedural measures

- Procedures for the realization, management and maintenance of assets
- Contingency/Recovery Procedures, based on the contingency scenarios that have been defined
- Training, awareness and capacity building procedures
- Operating procedures for monitoring, supervision and evaluation/audit
- Procedures for access management
- Procedure for carrying out water quality analysis
- Operational procedures for security personnel (functions, schedules, staffing, etc.).
- Incident management and response procedures
- Procedures for performing and testing backups.
- Procedure for managing users and credentials.
- Equipment hardening procedures.
- Vulnerability management procedures.
- Conducting periodic cybersecurity assessments on industrial systems.
- Procedures for managing the work of third parties.

6.3 Protective or Technical Measures.

6.3.1 Preventive measures:

The content of this section is restricted.

6.3.2 Detection Measures:

The content of this section has been limited.

- Physical risks.
  - Intrusion detectors, video surveillance cameras / CCTV
  - Measures for package control and detection of toxic substances, explosives, etc.
  - License plate readers
  - Temperature detector and mask in a health pandemic situation.
  - Early detection of the incident through video surveillance and intrusion sensors at access points.
  - Opening and tampering detectors for control panels.
  - Provide warning and alarm systems for responsible persons in the event of movements in drainage organs.
  - Intercommunication with the State Security Forces and Corps (FCS).

- Cybersecurity risks
  - Anti-malware protection.
  - Deployment of monitoring systems (intrusion detection systems, both on the network and on NIDS/HIDS clients; log collection systems, etc.)

6.3.3 Coordination and Monitoring:

- Security Control Center (alarm control, image reception and viewing, etc.).
- Logical security operations center (may also be included in the above).
- Surveillance teams (shifts, rounds, volume, etc.).
- Communication systems

7 PROPOSAL FOR IMPROVEMENTS

The road ahead for the protection of strategic hydraulic infrastructures is arduous and we cannot complete its implementation in a few years. It is logical to think that the implementation of a new way of acting will require several decades to be able to carry it out, especially if we consider how long it is taking us to implement the Emergency Plans

for Dams and Ponds, whose first basic civil protection guideline was from 1995 and which we are still working on today.

The COVID-19 pandemic has revealed society's weakness in the face of viruses with national or universal effects. It has demonstrated the great vulnerability caused by airborne transmission and has turned water into an essential hygienic tool in the fight against the virus. We have also learned that wastewater analysis becomes a precursor-detector of the beginning of the pandemic. Once again, the strategic and critical importance of this essential service has been demonstrated.

Below are some ideas from the Water Sector that we will need to work on in the coming years or decades.

- Disinvestment in the water sector.
  In the last decade in Spain, investment in water infrastructure has stopped, both from the private and public sectors. This is causing a constant and massive loss of human resources, an aging of the workforce and a deficient economic investment in maintenance and operation, which hinders management and, above all, the safety of the infrastructure.
  The causes are motivated by the economic crisis and public debt, a change in investment criteria betting on other renewable energies, abandoning hydraulic energy, and less public control due to the shortage of civil servants who can require it. Workers in the water sector are increasingly fewer, more generic, have less experience, have less public controls that require them to take measures, when they request them, investments do not arrive and their workday tasks are increasingly greater.

  The private sector, which is much more agile in adapting to this phenomenon of human resource restrictions, has promoted increasing automation and centralization of resources. This is undoubtedly an advantage in some aspects, but it also has its disadvantages:
    - Problems in case of failure to operate “in manual mode”.
    - Greater difficulty in reacting quickly to failure.
    - Need for much more specialized personnel, more difficult to train and replace.
    - Facilities without human presence for long periods of time are much easier to sabotage.
    - In the field of dams, there is an exodus of civil engineering professionals to other sectors and a predominance of industrial specialisation, promoting production over safety.

- Legislative measures.
    - Implementation of legal protection frameworks. There is a lack of protection against information sabotage (disinformation, fake news, discrediting) which, in an aspect as transcendental from a health point of view as water, can create a significant social alarm. The right to

information and freedom of the press are rules of coexistence that we have imposed on ourselves in democratic countries, but perhaps the mass transmission of unverified or unreliable information, the elimination of fake news on social networks, or the insertion of an additional text indicating it could be regulated. Without a doubt, the issuance of homogeneous and contracted official data always helps to avoid misinterpretations, so it seems important to establish standard protocols for the issuance of official data.

- Homogeneous legal frameworks. Dam regulations have not been homogeneous in the past, some dams have been subject to the Regulation and others to the Instruction, with different final criteria. The final approval of the Technical Safety Standards, by Royal Decree 264/2021 of April 13, has undoubtedly been a great help, but now their actual adaptation remains.
- In some autonomous communities there is still no regulatory body for the safety of dams and reservoirs outside public waterways.

- Integration of legislative measures into organizations.
  Most companies in the water sector have incorporated the new safety management procedures (Operator Safety Plan, Specific Protection Plan, Operational Support Plan and their revisions) and the new organizational figures in their staff (Safety and Liaison Officer and Safety Delegate) into their structures. However, the actual implementation of these new legislative standards is having a lower degree of compliance in the administration. On the one hand, the new functions, competences and responsibilities of the Safety and Liaison Officer and the Safety Delegate require a modification of the Administration's Job List, where, for example, the need to have the qualification of a Safety Director should be noted, as established by Law 8/2011, of 18 April, which establishes measures for the protection of critical infrastructures, and possibly incentivize their access with better specific complements. On the other hand, the new management procedures require investment to be able to implement them.

- Complexity and interdependence with other strategic sectors.
  The Supply Chain Subsector is highly fragmented. This can be an advantage for criticality purposes because not many users are affected in the event of a failure. However, it is also a disadvantage, because it is much more difficult to foresee a vulnerability and more difficult to protect against it.

- Strengthen and promote the relationship between dam owners and the State Security Forces and Corps (FCS).
  To enhance the great willingness and professionalism of the FCS that have always responded to the requirements of the operators, by holding training sessions, drills, technical visits to the facilities, etc.

8 ANNEX I: CATALOGUE OF THREATS

Category	Code	Threat
Specific cybersecurity risks	CYB.1	Interference in monitoring software: encryption of real-time servers, unauthorized access to monitoring or management interfaces…
	CYB.2	Interference in network and communications electronics: modification of network settings, etc.
	CYB.3	Communications interference: Man-in-the-Middle attacks, etc.
	CYB.4	Interference at the control level: carrying out improper operations, unpredictable system operation, falsification of information received by operators, activation/inhibition of alarms, etc.
	CYB.5	Interference with instrumentation: for example, modification of sensor configuration/calibration.
	CYB.6	Interference in actuators: modification of configurations, start/stop orders for pumps, opening/closing of gates, etc.
Accidents, interdependencies and operational and technical risks	ACC.1	Transport accident
	ACC.2	Technical failure
	ACC.3	Accidental risks
Terrorism and organized crime	TER.1	Explosives in suicidal people
	TER.2	Explosives in manned ground vehicles
	TER.3	Explosives in unmanned ground vehicles
	TER.4	Explosives in unmanned aircraft
	TER.5	Explosives in boats or unmanned vessels
	TER.6	Explosives in boats or manned boats
	TER.7	Explosives in stopped vehicles
	TER.8	Explosives in packages sent by mail
	TER.9	Explosives placed or abandoned
	TER.10	Grenade/mortar launcher attacks

	TER.11	Armed terrorist attack
	TER.12	Mass poisoning
	TER.13	Chemical attack
	TER.14	Radiological attack
	TER.15	Nuclear attack
	TER.16	Arson
	TER.17	Electromagnetic pulse
Aggressive crimes	CRA.1	Assault and extortion
	CRA.2	Sabotage
	CRA.3	Bomb threat
Ordinary crime	DEL.1	Heist
	DEL.2	Theft
	DEL.3	Fraud
	DEL.4	Vandalism
	DEL.5	Illegal Occupation
Meteorological risks	MET.1	Floods
	MET.2	Fires
	MET.3	Storm
	MET.4	Thunderstorm
	MET.5	Electromagnetic pollution
	MET.6	Storm surge
	MET.7	Hurricanes
	MET.8	Tornadoes
	MET.9	Heat wave
	MET.10	Cold snap
	MET.11	Drought
	MET.12	Snow
	MET.13	Hail
	MET.14	Ice
Geophysical risks	GEO.1	Earthquakes
	GEO.2	Tsunamis
	GEO.3	Volcanic eruption

	GEO.4	Sinkings
	GEO.5	Landslide
	GEO.6	Geomagnetic storm
	GEO.7	Meteorites
Threats of terrorist or malicious origin	ETM.1	Malicious activation of floodgates
	ETM.2	Broken pipes
	ETM.3	Use of explosives in floodgates
	ETM.4	Blasting or serious damage to dam elements
	ETM.5	Blockage in air ducts
	ETM.6	Drainage manipulation
	ETM.7	Intentional contamination of reservoir water
	ETM.8	Intentional air pollution in galleries
Threats to structural or internal security	ESI.1	Access road cut
	ESI.2	Avenues
	ESI.3	Waves in the reservoir
	ESI.4	Freeze-thaw cycles
	ESI.5	Unforeseen loads on the dam
	ESI.6	Upstream dam failure
	ESI.7	Fall of large objects into the reservoir
	ESI.8	Earthquake
	ESI.9	Persistent power line outage
	ESI.10	Persistent communications outage
	ESI.11	Pluviometric and hydrological conditions according to seasonality
Loose material bodies of prey	EMS.1	Rip-rap degradation
	EMS.2	Malfunctioning drainage system
	EMS.3	Clogged drains and filters
	EMS.4	Biointrusion
	EMS.5	Shallow gully
	EMS.6	Temporary saturation of the downstream backfill
	EMS.7	Opening of cavities or sinkholes

	EMS.8	Overpressures in contacts between rigid structures and embankments
	EMS.9	Differential movements
	EMS.10	Load transfer
	EMS.11	Internal erosion (Uplift)
	EMS.12	Liquefaction
	EMS.13	Uplift
	EMS.14	Upstream sliding
	EMS.15	Downstream sliding
	EMS.16	Breakage in pipes inside the dam
	EMS.17	Abnormal flow in conduits inside the dam
	EMS.18	Overflow
	EMS.19	High flow filtration
Factory dam bodies	EPF.1	Cracks and fissures
	EPF.2	Misalignments
	EPF.3	Differential movements
	EPF.4	Deformations
	EPF.5	Material degradation
	EPF.6	Overpressures
	EPF.7	Overturned
	EPF.8	Generalized obstruction of drains
	EPF.9	Block slide
	EPF.10	Significant flow filtration in the dam body
	EPF.11	Corrosion
Foundations	ERC.1	Foundation movements
	ERC.2	Deformations and settlements
	ERC.3	Internal erosion (piping)
	ERC.4	Degradation
	ERC.5	Swelling
	ERC.6	Liquefaction
	ERC.7	Opening of cavities
	ERC.8	Sinkholes

	ERC.9	Cavity collapse
	ERC.10	Ice cream with fillings
	ERC.11	Undermining
	ERC.12	Uplift
	ERC.13	Foundation erosion,
	ERC.14	Significant flow filtration in foundations or abutments
Reservoir	EMB.1	Saturation of the reservoir slopes
	EMB.2	Large landslides
	EMB.3	Waves in the reservoir caused by landslides
	EMB.4	New filtration pathways in the glass
	EMB.5	Formation of vortices on the water surface or sinkholes
	EMB.6	Reservoir silting up
Facilities	EIN.1	Loss of control of the dam
	EIN.2	Isolation of the dam
	EIN.3	Incorrect valve handling
	EIN.4	Incorrect handling of gates
	EIN.5	Destruction of valves of drainage organs
	EIN.6	Deterioration of valves of the drainage organs
	EIN.7	Destruction of the gates of the drainage organs
	EIN.8	Deterioration of the gates of the drainage organs
Industrial origin	EOI.1	Electromagnetic emissions
	EOI.2	Fault
	EOI.3	Denial of service by third parties
	EOI.4	Power failure
Polluting activities	EAC.1	Illegal dumping sites in the basin
	EAC.2	Illegal dumping into water bodies
Navigation	ENA.1	Damage to derived socio-economic uses
	ENA.2	Damage to fragile aquatic ecosystems
Undue human activity	EHI.1	Unauthorized access

	EHI.2	Unauthorized controls
	EHI.3	Disclosure of sensitive or classified information
	EHI.4	User errors
	EHI.5	Destruction of information
	EHI.6	Loss of information
	EHI.7	Sabotage by the organization's own personnel.
	EHI.8	Kidnapping, bribery or extortion of a worker by forcing him to commit sabotage against his will
	EHI.9	Incorrect handling of system operations
	EHI.10	Incorrect handling of hydraulic retention facilities
System failures	EFS.1	Persistent failure of the operating system
	EFS.2	Persistent failures of the auscultation system
	EFS.3	Persistent failures of security systems

Table 18Threat Catalogue.