IDM UID
TZYDJH
VERSION CREATED ON / VERSION / STATUS
17 Feb 2026 / 2.5 / Approved
EXTERNAL REFERENCE / VERSION

MQP Level 2

MQP L2 Physical Security Protection Management Procedure

Document describing the General Physical Security of the ITER Site

Approval Process			
	Name	*Action*	*Job Title / Affiliation*
Author	**Zingraff L.**	**17 Feb 2026:signed**	**Nuclear security engineer**
Co-Authors			
Reviewers	**Peaucelle X.** **Perrier G.**	**17 Feb 2026:recommended** **18 Feb 2026:recommended**	**Section Leader** **Head of Department**
Approver	**Barabaschi P.**	**27 Feb 2026:approved**	**Director-General**
Information Protection Level: Non-Public - Unclassified *RO: Jung Hwanmo*			
Read Access	**GG: MAC Members and Experts, AD: ITER, AD: External Collaborators, AD: External Management Advisory Board, AD: OBS - Security and Safety Section (SES), AD: Nuclear Safety Inspectors, AD: OBS - Quality Management Division (QMD), AD: DA, AD: Auditors, AD: ITER Management Assessor, project administrato...**		

#drn#

Change Log			
MQP L2 Physical Security Protection Management Procedure (TZYDJH)			
Version	***Latest Status***	***Issue Date***	***Description of Change***
v0.0	In Work	25 Oct 2016	
v1.0	Signed	08 Jan 2018	First issue. Document created as per MQP doc Request US8JNX
v1.1	Approved	09 Feb 2018	Integration of comments
v2.0	Signed	20 Apr 2020	As per approved MQP doc Request - 2WLT5K, the list of main changes is: * update the abbreviations after Re-org * add references 29 to 40 to structure the document * update the flow chart and description of the new steps to include the management of request to modify Security System (chapter 6.4) * add chapter 6.2.1.1 Site Boundary fence * add chapter 6.2.4.3 Forbidden items on site and search * add chapter 6.2.8 Drone utilization * update the outputs chapter The word file with tracked changes is attached to the MQP doc Request - 2WLT5K.
v2.1	Signed	25 May 2020	Integration of Tim Luce's comments.
v2.2	Approved	10 Jun 2020	This new version integrates a definition of "physical security" as suggested by T. Luce.
v2.3	Signed	01 Dec 2025	Minor updates to include Authorization related to the activities of possession, use, transfer and import of nuclear materials Changes: - updated acronym as per IO organizational changes - reinforced photography and videography activities on the ITER site - added security culture for the protection of nuclear materials
v2.4	Signed	18 Dec 2025	IDM technical issue
v2.5	Approved	17 Feb 2026	addition of the mention of the exclusion of Corbières

Table of Contents

1 PURPOSE 2
2 SCOPE 2
3 BASIC PRINCIPLES 2
4 FLOW CHART 4
4.1 PHYSICAL SECURITY OBJECTIVES 5
4.2 PHYSICAL SECURITY SYSTEM 5
4.3 ANALYSE AND EVALUATION 9
4.4 MODIFICATION OF IO'S PHYSICAL SECURITY SYSTEM 10
4.5 SECURITY CULTURE 10
5 RESPONSIBILITIES 11
5.1 DIRECTOR-GENERAL 11
5.2 SAFETY AND QUALITY DEPARTMENT (SDQ) AND THE SECURITY AND SAFETY (SES) SECTION 11
5.3 SCZ'S RESPONSIBLE OFFICER & STAFF MEMBERS ROLES AND RESPONSIBILITIES 12
5.4 ON-CALL DUTY FOR SECURITY INSIDE THE SES SECTION 12
6 LINK WITH OTHER PROCESSES 12
6.1 INTERACTIONS WITH NUCLEAR SAFETY PROCESS 12
6.2 INTERACTIONS WITH THE ENVIRONMENTAL PROTECTION PROCESS 12
6.3 INTERACTIONS WITH HUMAN RESOURCE PROCESSES 12
6.4 INTERACTIONS WITH IT PROCESS 12
6.5 INTERACTION WITH DESIGN CONTROL PROCESS 13
6.6 INTERACTION WITH QUALITY ASSURANCE PROCESS 13
7 OUTPUTS 14
8 DEFINITIONS AND ACRONYMS 15
8.1 DEFINITIONS 15
8.2 ABBREVIATIONS 15
9 APPLICABLE AND REFERENCES DOCUMENTS 15
9.1 APPLICABLE DOCUMENTS 15
9.2 REFERENCE DOCUMENTS 16

1 Purpose

The physical security of the ITER Site is fundamental for the ITER Organization and the success of the ITER Project.

The purpose of this document is to define the physical security management requirements for the ITER Site. These physical security management requirements establish the fundamental principles to be applied, specify the target security objectives and determine the different responsibilities in this field. This document also lays out a set of permanent measures that must be complied with in order to reach these security objectives.

Site protection is everyone's responsibility and each person present on the ITER Site shall comply with these physical security management requirements.

These physical security management requirements must be checked and updated regularly to take into account any changes to the ITER Project, the threat levels and the applicable laws and regulations [3][5].

2 Scope

This document, Level 2, belongs to the ISMS [9] in the scope of the Security process.

The physical security management requirements apply to the physical security of the ITER Site in its entirety and this regardless of the state of progress of the ITER Project.

The physical security management requirements shall be complied by:

- Any legal person taking part in the design, construction or operation of a facility, or performing any service on the ITER Site,
- Any person who has a legitimate reason for being present on the ITER Site and thus provided with site access rights.

This document does not apply to Corbières.

Any physical security systems and components, including those delivered by PBS 69, are under the exclusive responsibility of the SES section.

IT measures to ensure the availability, confidentiality and integrity of the information system contributing to the physical protection system and related data are not encompassed in this document but in [12].

3 Basic principles

The physical security objectives are achieved when the following physical security management requirements are applied, where economically and technically achievable, on the ITER Site.

- IO measures for physical security shall be based on a graded approach, taking into account an evaluation of the threat, the relative attractiveness of potential targets, the nature of the present or future targets and potential consequences associated with malevolent acts in accordance with Host State related regulations.
- The IO's physical security system shall be guaranteed by deploying several lines of protection which form a defence-in-depth system and which shall rely on the following key factors:
  - Technical, human and organisational means ensuring an access control system.
  - Early detection and delay[1], video surveillance system, alarm assessment and communications system.
  - Immediate response executed by permanent guards on site and, if needed, Host State response forces.

[1] For a system to be effective at this objective there must be awareness that there is an attack (detection) and slowing of adversary progress to the targets (delay).

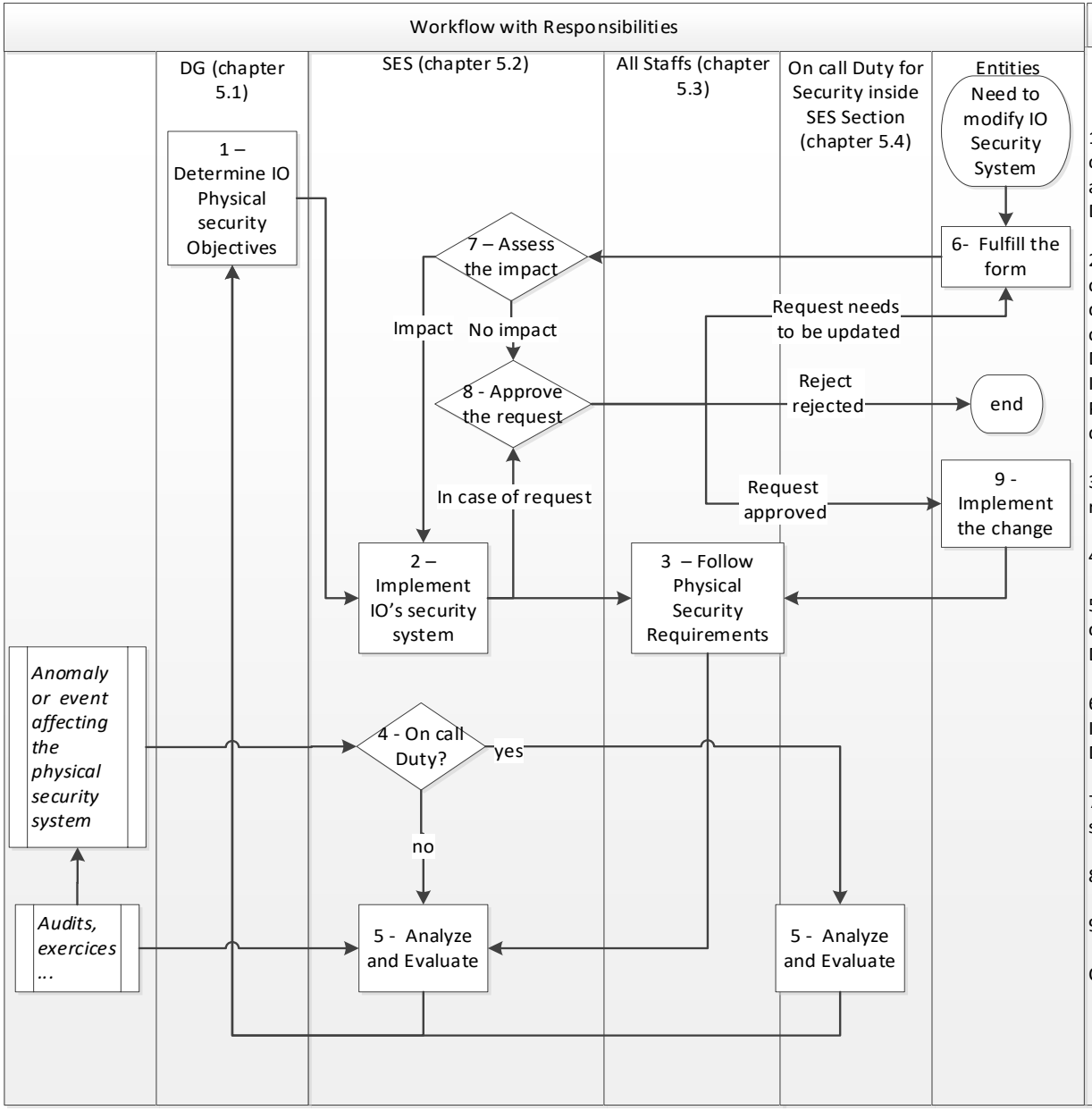
- Limited access to sensitive information to those whose trustworthiness, appropriate to the sensitivity of the information, has been established and who need to have access to such information for the performance of their duties.
- Update maintenance, repair and calibration of equipment as well as performance testing, operational monitoring and associated documentation management.
- The enhancement of the security culture.

The IO's physical security system is established on the basis of Host State regulations related to the protection of nuclear materials.

The IO has the formal authorization to store, use, manage, import and handle nuclear materials under the Host State nuclear material related regulation in the conditions detailed in [10]. These conditions shall be largely known by IO concerned entities (see section C). Details of the cooperation between the IO and the Host State security authority are mentioned in [11].

4 Flow chart

The following flow chart is a logical overview for applying these physical security management requirements.



Description of the step

1 - to determine the objectives of the physical security system by characterizing and defining the threats, by identifying the targets and performing a risk assessment
Details in chapter 4.1

2 – to implement the physical security system which relies on a combination of elements such as access control system, intrusion detection system (fences, sensors), procedures, CCTV system, communication devices (and associated maintenances) and guards.
Details in chapter 4.2
Interactions with other process Nuclear Safety / Environmental Protection / Human Resources / IT / Design Control / QA are defined in chapter 6

3 – to execute work according to physical security system requirements defined in this procedure

4- On call Duty service as defined in 4.2.2.3

5 – to analyse and evaluate this physical security system in order to continuously improve the management of physical security system.
Details in chapter 4.3

6 – to fulfill the appropriate form to request any modification of the IO physical security system
Details in chapter 4.4

7 – to assess the impact of the request, including if the IO's physical security system needs to be modified.

8 – to review and accept the request.

9 – to implement the change as defined in the approved request

Output of the execution of this workflow are described in Chapter 7

4.1 Physical security objectives

The ITER physical security system's main objectives are:

- Permanently protecting persons, assets and activities, hereafter so called “targets” on the ITER Site from any malevolent act.
  It is IO’s responsibility to identify the targets of concern. These may be Host State level targets such as nuclear materials or sources of ionising radiation, processing facilities, and storage facilities.
  A working instruction presents how to identify targets [14] and how to perform a security risk assessment. The Area Physical Protection Risk Assessment shall be approved by the Security & Safety Section Leader.
- Mitigating or minimizing the effects of a malevolent act and facilitating the return to normal after such an event.
- Achieving the protection objectives related to the threat assessment in partnership with specialized authorities of the Host State.
  Threat assessment consists of a comprehensive compilation of information about all potential adversaries and their motivation, intentions and capabilities.
- Fulfilling the relevant physical protection obligations prescribed by laws and regulations of the Host State in the field of protection against malevolent acts in compliance with Articles 14 and 20 of the above-mentioned Agreement [1].
- Ensuring the sustainability of the ITER physical security system with preventive and corrective maintenances and the enhancement of a security culture.

4.2 Physical Security System

Following this risk assessment, IO deploys technical and human means and an organization associated with procedures to ensure a physical security system. These main means and associated rules are listed hereafter and implemented on the ITER Site:

4.2.1 Technical means

4.2.1.1 Site boundary fence

The site boundary fence is under the exclusive responsibility of the SES section, which ensures its maintenance. The patrol road along the site boundary fence is reserved for security purposes, and it is not authorized to have a walking tour along the site boundary fence.

The document [15] lists the interface between SES section and BSM/BFO.

4.2.1.2 Access Control System (ACS)

The electronic access control system (ACS) applies to the detection and prevention of entry of undesired individuals into the ITER Site, an area, a building, or a sensitive room.

The operational management of this electronic system is under the exclusive responsibility of SES section. Rules of use, operating procedures, and record archiving duration are detailed in [16]. The actions performed by the different system users must be traceable.

4.2.1.3 Closed-Circuit Television (CCTV) – Video Surveillance

A video surveillance system is implemented on the ITER Site for the security of people and goods. The main functions of this system are:

- Dissuasion.
- Contributing to Site surveillance.
- Determining the origin of the malevolent act.
- Detecting an intrusion.
- Dispelling any doubts.

- Assisting in the control of flows (vehicles and people).

The operational management of this video surveillance system is under the exclusive responsibility of SES section. Rules of use, access rights, operating procedures, and record archiving duration are detailed in [16]. The actions performed by the different system users must be traceable.

The procedure [17] details how other video systems installed on the ITER site shall be managed.

4.2.1.4 Communication systems

Dedicated, redundant, and diversified communication systems are installed for site protection actions and exchanges with Host State authorities and other relevant entities.

The procedure [18] details how the radio system installed on the ITER site shall be managed.

4.2.1.5 Protection of physical protection IT systems

The physical security IT systems (e.g., access control system, CCTV system) are dedicated to physical protection and are not connected to a public network.

The physical security IT systems are provided with a level of protection equivalent to that required for the equipment and functions that they protect.

Provisions are to be made to detect any fraud concerning these systems, as well as any deterioration of their performance, with the support of IO/IT, as detailed in [19].

Back-up power supply solutions are implemented for rooms, systems, and devices which are to guarantee the operational continuity of these security physical systems. However, such solutions are not required for power supplies whose failure does not affect the operating conditions of the above-mentioned equipment and devices.

In addition, provisions must be made to guarantee the confidentiality and integrity of the physical protection IT systems of the ITER Site and related data, as defined in [12].

4.2.1.6 Maintenance

All technical components of the physical security system shall be subject to acceptance certificates and to an exhaustive and periodical control, called maintenances, eventually completed by unannounced tests.

Maintenances are performed by SES section staff and external contractors in accordance with [20].

The objectives of these maintenances are to ensure that the ITER physical security system and the respective system components comply with the expectations and requirements from all aspects. The maintenance program also provides a high degree of confidence that degradation is identified and corrected.

For any physical security components or system, a maintenance program including preventive and corrective maintenance and a performance-testing shall be established.

These controls are ruled by procedures, traced (preventive and corrective reports), archived and managed in accordance with confidentiality rules [21].

4.2.2 Human Resources

4.2.2.1 Guarding service

Under the responsibility of SES section, a Guarding service is provided 24 hours a day, seven days a week. The main objectives are:

- To check that only authorized persons have access to the different areas of the ITER Site, and in accordance with internal regulations [22].
- To ensure the protection of the facilities, property, employees, contractors, and visitors of the ITER Site against malevolent actions.

4.2.2.2 Security Command Post

A Security Command Post is set up and is permanently manned by security personnel of the guarding service who ensure the following tasks (see [23] for more details):

- Collect and display permanently in real time information and alarms which can result in damage to the ITER property, employees, population, or environment.
- Centralize urgent calls raised from the whole ITER site.
- Communicate with the local Host State's authorities in respect of [6].
- Communicate with IO on-call staff members, operational teams, other relevant Control Rooms, and the Cadarache CEA/FLS in accordance with [24].
- Assess and process all alarms in the field of safety and physical security.

Only a limited number of duly authorised people are allowed to access the Security Command Post as defined in [25].

4.2.2.3 On-call security service

An on-call security service is ensured by the designated SES section staff members in accordance with [26][27] according to a defined calendar [28].

4.2.3 Organization and procedures

The defence-in-depth of the targets will be ensured by the implementation of several Security Controlled Zones (SCZ) and associated requirements defined in [29]. Following the risk assessment, a scalable level of protection from unauthorised or covert access, and forcible attack shall apply for each SCZ.

The definition of SCZ is linked to the impact of the compromise, loss of integrity, or unavailability of the information and assets inside the SCZ in accordance with the risk assessment matrix detailed in [12][14] from low to very high.

SCZ could be buildings, rooms, and fenced areas in which access and traffic are both regulated and restricted to deter and prevent anyone from entering to commit a malevolent act.

Multiple layers of protection will provide IO with a greater delay, allowing a response to any unauthorized entry.

SES section is responsible for deploying the measures needed to protect the ITER Site and SCZs in line with applicable legal provisions or with an appropriate level of protection based on the type of activity performed in the facility, the threat identified, and the associated risks in the case of a malevolent act. The resulting Security Instructions and Security Plan (plan de protection) shall be approved by the Security & Safety Section Leader.

SES section ensures the strict monitoring of the physical protection devices and systems deployed in these SCZ.

4.2.4 Accessing the Site and SCZ

4.2.4.1 Background check

Any person requesting an ITER Site access may be subject to a background check by the Host State's relevant Authorities under the provisions of the French Defense Code [3]. Background check conditions are detailed in [30].

The IO has the authority to refuse or withdraw any access at any time for safety or security reasons.

4.2.4.2 Access authorizations, badges, and rights

In addition to the ITER Site access authorization issued in accordance with [30], anyone accessing an SCZ shall have a name-based badge which can be checked before entering the relevant SCZ. The badge conditions defined in [31] shall be followed. This badge must be visibly worn at all times. In case of dangerous works, the badge must be in the pocket.

Any person responsible for an area or a building shall detail access rules for the said area or building, following the template [32].

Rules for accessing, driving, and parking vehicles on the Site defined in [33] shall be followed.

Specific security requirements for organizing events, workshop or conferences detailed here Workshop Organization Best Practices - Workshop Organization - ITER Intranet shall be followed.

4.2.4.3 Forbidden items on site and search

The DG may authorize security controls to be carried out on the ITER Site.

All offices, buildings, areas, and vehicles entering or present on the ITER Site may be subject to security controls detailed in [34].

List of prohibited items on the ITER Sites without prior written authorization from the DG is detailed in the Internal regulations [22].

All valuable objects and documents needing special protection shall be stored and locked before leaving the office.

4.2.5 Staff awareness and training

Anyone present on site must be aware of the security issues. The staff members must know their obligations regarding these issues and regarding the potential threats to the ITER Site.

Provisions must be made, under the responsibility of SQD/SES, and, when relevant, in liaison with the HRD [35] to ensure that awareness programmes are organised as soon as the staff members and workers take on their duties. Staff members and workers must be fully aware that a credible threat exists and that the role of the individual is important.

IO entities engaged in the protection of nuclear materials and radiological shall receive additional training that contains at least the elements of required security measures, Host State regulations, how to respond to a security event, and security awareness.

4.2.6 Key management

SES section is responsible for the safekeeping, management, and tracking of Gate keys, Building access badges, and Keys to sensitive rooms.

The other keys are kept, managed, and tracked by BFO as defined in [36].

4.2.7 Taking photos and filming on-site

Photography and videography activities are key component of the communication strategy of the ITER Organization to generate understanding of and support for the ITER Project among ITER stakeholders and the general public. It can also support technical aspects of construction, maintenance, facility, or logistics aspects.

Taking photos and filming is permitted on the ITER Site but some restrictions apply as detailed in [Ref.55].

It is reminded that CEA Cadarache center's fences and facilities shall not be neither photographed nor filmed.

Aerial photography and videography of the ITER site shall follow the process described in [37].

4.2.8 Indoor & outdoor flight

Operations requiring a flight indoors or in the airspace above the ITER Site shall be done and prepared in accordance with the instructions detailed in [37] in order to comply with Host State regulation [8].

4.2.9 Protecting information related to the physical security system

The Site's physical security system covers the human resources aspects, the procedures, the security systems, and the equipment. Certain information on this system is public and aims to inform any person accessing the Site about the relevant protection measures and to increase the awareness of all persons in relation to security issues. Other information, including all of the details required to implement the physical security system, must be protected and shall only be shared with people who have a need-to-know in relation to their activity, as detailed in [29]. The most sensitive information shall be classified on the basis of [4] and shall only be shared with people who have a need–to-know in relation to their activity and who have been approved by the French authorities.

All of the people working on the different components of the physical security system during the various phases of its life cycle (design, operation, maintenance, and removal) shall make sure that this information is correctly protected.

4.3 Analyse and Evaluation

4.3.1 Anomalies and events affecting the physical protection system

Failure to observe the requirements of the ITER physical security system shall lead to measures to be decided by the DG or SQD Head, or his delegate, in liaison with the SES section. It may include disciplinary measures for staff members or equivalent measures for non-staff members, in particular suspension/exclusion of access to the ITER site in accordance with [38][49].

Any anomaly affecting the physical security system requiring the implementation of compensatory measures, or the detection of an event likely to affect the protection of the Site and its facilities is subject to an immediate declaration first to the Command Post who will report to Security and Safety Section Leader that will escalate it to SQD Head and, if applicable to DG and to the relevant authorities of the Host State using the reports forms detailed in [39] and within the appropriate timescale. This declaration could be completed by a report [40] specifying the measures taken. When applicable, the area owner shall be informed by the SES section of the physical security event and about the compensatory measures taken. The Security Report shall be approved by the Security and Safety Section Leader.

The procedures [23] and [41] detail the organisation and responsibilities of IO in the event of a serious incident or accident, within either the ITER or CEA premises, which might require immediate actions, in order to protect the Site or the image of the ITER Organization.

This procedure provides response mechanisms for different crisis scenarios and therefore covers all emergency situations. An additional specific emergency response plan might be elaborated.

4.3.2 Audits

Audits to assess the execution of this procedure can be performed on management request by using [42].

4.3.3 Exercises

The SES section conducts regular exercises [43] to assess and validate the contingency plans and also to train the various participants on how to react in such a situation (e.g., coordination between the guards and response forces, with crisis cells). These exercises are subject to reports that summarize the observations made, the lessons learned, and the improvements to be implemented. The Security Report shall be reviewed by the Security & Safety Section Leader.

Host State's security response forces shall be involved in an exercise at least once a year.

4.4 Modification of IO's Physical Security System

A Change Requestor, such as an area owner, can request a modification of the ITER's physical security system by adding fences, badge readers, or security cameras.

Before any modification, the Change Requestor shall liaise with the SES section, which shall assess if the IO's physical security system needs to be modified in accordance with the risk analysis mentioned in 4.2.3. The implementation of the modification is subject to the SES section leader's approval.

In some cases, and in accordance with [10] the SES section needs to inform (one-month deadline) the Host State security authority or to request formal authorization (three-month deadline).

4.5 Security culture

According to [9], the IO security culture is based on the collective awareness (of individuals directly or indirectly involved in the protection of nuclear materials) that security is a priority, the awareness of the sensitivity of the activities performed, and the existence of a credible threat.

To maintain and develop this safety culture, the ITER Organization relies on:

- A formalized organization for the protection and control of nuclear materials and sources of ionising radiation, detailed in [44];
- A clear description of responsibilities and roles of each stakeholder involved in nuclear security;
- Significant investment in training and qualification of personnel involved;
- Strong involvement of operational staff in the selection of protection measures;
- Control of access to sensitive information and awareness among all personnel about the importance of this control (awareness through functional relays, security officers, and information systems security agents);
- A concept of operational readiness maintenance, ensuring that the operation and maintenance of devices contributing to the protection and control of nuclear materials and sources of ionising radiation are maintained so that their function is not compromised, with contingency measures in place if necessary;
- Implementation of inspections (by authorities, senior management, and the SES section);
- Conducting security exercises;
- Rigorous handling of anomalies, malfunctions, or deficiencies identified;
- Personnel's knowledge and compliance with internal procedures and regulations;
- Regular awareness of the ITER Site personnel regarding the challenges of nuclear materials and sources of ionising radiation protection and control, as well as awareness among new arrivals at the ITER Organization and external companies working on the site;
- Security requirements from the ITER Organization in its dealings with contractor companies.

This comprehensive approach underscores the ITER Organization's commitment to ensuring security in its operations, especially those involving nuclear materials and sources of ionising radiation.

5 Responsibilities

5.1 Director-General

The DG or his delegate (the Safety and Quality Department Head) is responsible for all safety and security matters and whenever Host State regulations must be observed. For these purposes, he cooperates and coordinates with all Host State entities that have physical protection responsibilities, such as off-site Host State response forces, in compliance with the ITER Agreement, the Agreement on the Privileges and Immunities of the IO and the Headquarters Agreement [2].

5.2 Safety and Quality Department (SDQ) and the Security and Safety (SES) section

The Safety and Quality Department must:

a) Check that the operating conditions of the ITER Site integrate physical security requirements, including crisis management.
b) Ensure that physical security obligations prescribed by applicable legal provisions of the Host State in the field of protection against malevolent acts are fulfilled.

To accomplish these tasks, the SES section is responsible for:

a) Performing a risk assessment in collaboration with relevant IO departments and offices on the basis of calculations of chemical or radiological consequences.
b) Defining and then ensuring the implementation of permanent and progressive protective measures, as well as the maintenance of the physical security system and its components.
c) Formalising the responsibilities and tasks of the people in charge of physical security, notably the guarding service (patrols and intervention) and the on-call security duty.
d) Analysing any incident impacting or detected by the physical security system, this includes identifying the causes, implementing compensatory measures, and defining corrective actions.
e) Defining the terms of access rights to the ITER Site, areas, facilities, and premises subject to the site access control procedure (including visitor tours in liaison with the Communication & External Relations team).
f) Monitoring staff members' awareness of the stakes in protecting the ITER Site.
g) Cooperating with the relevant Host State's authorities in all matters of protection and coordinating actions with the response teams (including emergency drills) in compliance with the ITER Agreement, the Agreement on the Privileges and Immunities of the IO and the Headquarters Agreement.

5.3 SCZ's responsible officer & staff members roles and responsibilities

Any responsible officer of an SCZ is responsible for the implementation of all security measures within the SCZ.

The IO line managers and IO contract managers, or their delegates, respectively, ensure that staff members and contractor personnel are aware of the security rules in force designed to protect people, the ITER Site, the facilities and assets, and that these rules are followed.

All badge holders with access to the ITER Site must quickly inform their hierarchy or the Command Post of any suspicious behaviour or event impacting or likely to impact the security of people or the ITER Site.

5.4 On-call duty for Security inside the SES section

As defined in [26][27] and reminded in 4.2.2.3, the on-call duty service is responsible for ensuring the continuity of service in case of:

- An anomaly affecting the physical protection system on the ITER Site;
- Detection of an event with a possible impact on the protection of the ITER Organization general premises/properties or identified sensitive targets on the ITER Site;
- Events affecting the security or safety of staff members and their families requiring immediate assistance in relation with the Minister of Interior's security forces;
- Any other relevant areas related to Security.

6 Link with other processes

6.1 Interactions with Nuclear Safety Process

One input for the execution of this MQP document is provided by the identification of nuclear materials and sources of ionising radiation located within the ITER Site (element, isotope, quantity, and irradiation) as defined in [45].

6.2 Interactions with the Environmental Protection Process

When a facility is designed to treat or store chemical, nuclear materials, or sources of ionising radiation or special components whose loss would lead to unacceptable damage in terms of delays or costs for the ITER project, the physical security system must be efficient against malevolent actions.

6.3 Interactions with Human Resource Processes

In liaison with the SQD and SES section, the HRD:

- Defines the administrative conditions applicable to the on-call security service as mentioned in section 4.2.2.3.
- Is responsible for scheduling awareness training for newcomers as defined in [35].

6.4 Interactions with IT Process

The IT section, and in particular the RSSI, provides support so that suitable provisions are applied to ensure the availability, confidentiality, and integrity of the information systems contributing to the physical security system, together with the related data [19].

6.5 Interaction with Design Control Process

The ITER technical departments are responsible for integrating security requirements into the design of the facilities, as defined in [46]. These departments shall provide:

- The physical security devices jointly defined with the SES section to reduce the risks of any identified threats.
- The emergency means designed to ensure the continued operation of the systems contributing to the Site's physical security.

Ensuring the security of the ITER Site facilities is an operational requirement. Therefore, the security needs shall be taken into account as early as the design phase of any facility. A risk assessment must be performed for any new building or facility and integrated into the design review. This risk assessment must be protected and only distributed to those with a need-to-know.

To avoid having multiple physical security systems on the ITER Site and to ensure that the security needs are taken into account in an overall and consistent manner, security devices must comply with the standards defined jointly with the SES section, as well as be incorporated into the existing overall system.

6.6 Interaction with Quality Assurance Process

The Level 2 MQP Procedure mentioned in paragraph 4.3.2 can be applied.

7 Outputs

Records related to Access Control are managed in accordance with [16] and are detailed in [30].
The execution of this document requires the following outputs:

Type of output	Format (Template, form, checklist)	Location of output	Document type	Instructions for the identification of the output	Responsible for managing the output	Retention period (1)
Paragraph 4.1: Risk assessment	Defined in [14]	Stored on a secure dedicated server	[SE]-Security Risk Assessment	The file name shall include the concerned area.	IO SES section Responsible officer	Until the decommissioning of the Site and facilities
Paragraph 4.2.1 Access reports	Defined in [30]					
Paragraph 4.2.5 Staff awareness	Defined in [35]					
Paragraph 4.2: Acceptance certificates for the various components of the physical security system which have been installed.	No specific format	Stored on a secure dedicated server	out of IDM	The file name shall include the name physical security system's component.	IO Security Technician assistant.	Until the decommissioning of the Site and facilities
Paragraph 4.2: Re-qualification documents for the physical security system in the event that one of its components is modified.	No specific format	Stored on a secure dedicated server	out of IDM	The file name shall include the name of the physical security system component and the date.	IO Responsible Officer for Reception Services	
Paragraph 4.2: All of the instructions or plan (plan de protection) related to the physical security system.	No specific format	In IDM	[SE]-Security Instructions [SE]-Security Plan	The file name shall explain the purpose, such as the Security Defence Scheme Building xxx.	IO Security Section Leader	
Paragraph 4.2: Preventive maintenance reports.	No specific format	Stored on a secure dedicated server	out of IDM Archived as a paper form.		IO Security Technician assistant.	
Paragraph 4.3.1 Declarations, general reports and anomaly or event analysis reports.	Defined in [40]	Stored on a secure dedicated server	[SE]-Security Report	The file name shall include the name of the event and the date and if applicable the physical security system component.	IO SES section Responsible officer	
Paragraph 4.3.1 Non conformity report	Defined in [54]					
Paragraph 4.3.2 Audit report	Defined in [42]					
Paragraph 4.3.3 Exercises report	Defined in [44]	Stored on a secure dedicated server	[SE]-Security Report	The file name shall include the name of the event and the date	IO SES section Responsible officer	Until the decommissioning of the Site and facilities
Paragraph 4.4 ''Term of use''	Defined in [48] and [37] for camera and indoor or outdoor flight. No specific format otherwise	Stored on a secure dedicated server	[SE]-Security Report	The file name shall explain the physical security system to be modified	IO SES Section Leader	

8 Definitions and acronyms

8.1 Definitions

- Physical security: describes security measures that are designed to deny unauthorized access to the ITER site and facilities, equipment and resources, and to protect personnel and property from malevolent acts. Physical security involves the use of multiple layers of interdependent systems that can include CCTV, ACS, security guards, protective barriers, perimeter intrusion detection and other technical, human and organizational means designed to sustain it (security culture, confidentiality, maintenance programme and response plan, information protection, …). [53]
- ITER Site - "ITER Site" refers to the configuration of the ITER Site as defined in the ITER Site Master Plan [13]

8.2 Abbreviations

- ACS: Access Control System
- BSM: Building & Site Management Program
- BFO: Buildings & Facilities Operations
- CEA: Commissariat à l'Energie Atomique et aux Energies Alternatives
- CCTV: Closed-Circuit Television
- CoSSeN: Commandement spécialisé pour la sécurité nucléaire
- DG: Director-General
- FLS: Formation Locale de Sécurité
- HRD: Human Resources Division
- IO: ITER Organization
- ISMS: Integrated Safety, Environment and Security Management System
- IT: Information Technology
- ODG: Office of the Director-General
- RSSI: (in French) Responsable de la Sécurité des Systèmes d'Information
- SCZ: Security Controlled Zones
- SES: Security and Safety

9 Applicable and References Documents

9.1 Applicable documents

[1] Agreement on the establishment of the ITER International Fusion Energy Organization for the Joint Implementation of the ITER Project signed on 21 November 2006 and effective on 24 October.

[2] Agreement on the Privileges and Immunities of the ITER Organization 2ET9RX

[3] French Defence Code Articles L.1332-1 and L.1333-1 and followings and Articles R. 1332-1 and R.1333-1 and followings.

[4] Instruction Générale Interministérielle n°1300 on the protection of French National Defence Secretary http://circulaire.legifrance.gouv.fr/pdf/2011/12/cir_34288.pdf.

[5] VIGIPIRATE plan.

[6] Decree No 2015-1533 of 25 November 2015 publishing the Additional Protocol, by exchange of letters, to the Headquarters Agreement of 7 November 2007 between the Government of the French Republic and the International Fusion Energy Organization for the Joint Implementation of the ITER Project regarding the French authorities' role in terms of their intervention for security purposes on the ITER Site, signed in Paris on 26 January 2015 and in Saint-Paul-lez-Durance on 10 March 2015.

[7] Decree No 2017-588 of 20 April 2017 creating a department with national competence within the ministry of interior and the ministry of energy named “Specialized Command for Nuclear Security” (CoSSeN in French).
[8] Arrêté du 22 janvier 2020 fixant la liste des zones interdites à la prise de vue aérienne par appareil photographique, cinématographique ou tout autre capteur
[9] ITER Integrated Safety, Environment and Security Management System (ISMS) Manual 4HCWJU
[10] Arrêté n° 003/2025 portant décision d'autorisation n° 003/2025 relative aux activités de détention, d'utilisation, de transfert et d'importation de matières nucléaires et aux activités nucléaires mettant en œuvre des sources de rayonnements ionisants au sein de l'établissement de !'Organisation Internationale ITER de Saint-Paul-lez-Durance
[11] Protocole relatif à la coopération entre le HFDS et ITER en matière de lutte contre la malveillance sur le site ITER” 5JU5CT

9.2 Reference documents

[12] Information Technology Security Policy 6GJKMH.
[13] ITER Site Master Plan 27X5FM
[14] Template for Security risk analysis - Storage facilities SSZV8D
[15] Technical interfaces between SD and CST LXSSY5
[16] SES data protection WT7JUL
[17] Work Instruction for the installation of camera system within the ITER Site 2FXFYG
[18] Conditions of Use of the ITER radio Communication System Y73ERA
[19] SHS request for service VL64UM
[20] SES Maintenance & Inspection plans 56JHZL
[21] Physical Protection Classification Guidance WMYGXF
[22] Internal regulations 27WDZW
[23] Emergency response alert procedure 7LB8NY
[24] Agreement on information modalities in the event of emergency situations between the ITER Organization and the Cadarache CEA Centre QEPH63
[25] B03 access procedure UQYJ3S
[26] Internal Administrative Circular No 18 - On-Call Duty Service 35GUGH
[27] Organization of the on-call duty for Security inside the Security, Health and Safety division QZ5DNP
[28] Public Holidays & Site closing dates 2V3KFB
[29] Physical protection security management requirements (security controlled zone and risk mitigation measures) VH7RZM
[30] ITER Site access procedure S3893D
[31] How to request access to and within the ITER Site WRWQRG
[32] Area Access "How-to" Template VH6TT9
[33] Vehicle Access and Traffic Circulation and Parking on the Site N3MG3V
[34] Procedure for security searches at ITER entrances YHFTFF
[35] Training plan process guidelines 2M3ZGV
[36] SHS Key management procedure VJPP23
[37] Flight authorization working instructions 4Y69MN
[38] ITER Site Protection Enforcement Rules V9ZWCA
[39] Host State reports form - 7T6S7R
[40] Physical Security Event Analysis 2TD6JW
[41] ITER General Emergency Procedure T24NPG
[42] Quality Management System Audits 2DQTA8
[43] Physical Protection exercise procedure T726F6
[44] GIN 035- Roles and Responsibilities for the Application of the Host State Regulations on Protection and Control of Nuclear Material and Protection of Radioactive Sources to the ITER Organization 8AZZDA

[45] Preliminary Safety Report 3ZR2NC
[46] Design Input Control Procedure U34CSG
[47] Template of the Terms of use for indoor & outdoor flight 2JMQXB
[48] ACS Concept of operations 89LYXJ
[49] CCTV Concept of operations 8A3EKG
[50] Report to Host State security authority 7T6S7R
[51] Protocole relatif à la coopération entre le HFDS et ITER en matière de lutte contre la malveillance sur le site ITER 5JU5CT.
[52] Background check instruction 87V4RF
[53] ITER security definitions 7GH8F5
[54] Procedure for Management of Nonconformities 22F53X
[55] On-Site Photography and Videography Procedure (F5V7F2)