

Technical scheme for the connected and communicating building



Acknowledgements

This scheme has benefited from the attention and expertise of numerous stakeholders.

Certivéa & Cerway wish to thank all players who were involved alongside it and who contributed to the conclusion of this project, starting with the Smart Buildings Alliance for Smart Cities (SBA) and the HQE-GBC Alliance for writing the technical requirements, the contributors to calls for comments, the participants in focus groups, the players in pilot projects and everyone representing the interested parties who were consulted.

Warning

The present document forms part of the labelling scheme for the R2S-Ready2Services label delivered by Cerway. It includes the whole of the scheme. However, in case of changes, only the content of the ISIA platform is authoritative for the labelling.

The "R2S-Ready2Services label" scheme is composed:

- Of labelling rules, which define the conditions under which the right to use the R2S-Ready2Services label may be delivered by Cerway.
- Of ISIA, Cerway's online digital platform for evaluating the R2S-Ready2Services approach.
- Of the usage charter for the mark "R2S-Ready2Services Label - delivered by Cerway".

The present document is protected by copyright.

Change history

Version number	Main modifications made
1.0	Creation and validation of the detailed technical scheme



Table of contents

Acknowledgements	2
Warning	2
Change history	2
Table des matières	4
Introduction	7
Context and objectives	7
Digital technology at the service of the building and its occupants	7
R2S label: technical resources for a high-performing and sustainable architecture	8
Main principles and definition framework of the Ready2Services label	9
The key principles of the Ready2Services approach:	9
The definition framework for the charter on the connected, socially-responsible and human-focused building	Erreur ! Signet non défini.
Scope of application	10
Perimeter of labelling	10
Commitment to a labelling process	10
Structure and scoring system	12
Structure of the scheme	12
Evaluation system	12
Identification	14
Labelling process	15
Key stages	15
ISIA, the online platform dedicated to R2S-Ready2Services labelling	15
Details of the requirements	16
Connectivity	17
Scale of points per requirement	18
CO1 - Connection to the building's external networks	21
CO1.1 Building prepared for connection to any type of external land line	21
CO1.2 Redundancy of the building's connection to all types of external land line	23
CO2 - Connectivity to land line networks	25
CO2.1 Cabling the building's general communication services	25
CO2.2 Preparation of cabling for the property units / activity areas of the building	26
CO3 - Connectivity to wireless networks	28
CO3.1 Nature and quality of the wireless networks	28

CO4 - Usability and scalability of the cabling	30
CO 4.1 Adaptability of the cabling distribution.....	30
CO5 - Redundancy and security of the cabling.....	32
CO5.1 Redundancy capacity of the building's cabling	32
CO5.2 Electrical power supply to the infrastructure.....	34
CO5.3 Access control and protection of infrastructure	36
Network architecture.....	37
Scale of points per requirement	38
RE1 - Smart Network and occupants' networks.....	41
RE1.1 Smart Network dedicated to the general services of the building	41
RE1.2 Networks dedicated to the communication services of occupants.....	42
RE1.3 Power supply to the communication terminals via the network.....	44
RE1.4 Support of the IPv6 protocol.....	46
RE2 - Continuity and functional protection of the Smart Network	47
RE2.1 Resilience capacity of the building's Smart Network.....	47
RE2.2 Detection of malfunctions and protection of the Smart Network	48
RE3 - Management of the Smart Network	49
RE 3.1 Administration of networks and their equipment	49
Equipment and interfaces.....	53
Scale of points per requirement	54
IN1 - Communication interfaces.....	56
IN1.1 Integration of the equipment of the building's Smart Network	56
IN1.2 Capacity of equipment to interface with the Smart Network through their APIs	57
IN2 - Openness of systems	59
IN2.1 Documentation and usage licences for the APIs	59
IN2.2 Integration in the digital model (BIM)	60
IN3 - Access to data and services	62
IN3.1 Procedures for access to data and to commands.....	62
IN3.2 Survival of the functions of communicating equipment	63
IN3.3 Stability of services.....	63
Digital security	65
Scale of points per requirement	66
SE1 - Security of networks and building systems	68
SE1.1 Authentication mechanisms to access to the Smart network	68
SE1.2 Conditional routing mechanisms of the Smart Network	70
SE1.3 Support for VLAN	71

SE1.4 Mechanisms for traffic monitoring and protection against malware	73
SE1.5 Encryption of communications	74
SE2 - Network security procedures	75
SE2.1 Monitoring flows and configurations of the Smart Network	75
SE2.2 Processing incidents and alert chain	76
SE2.3 Equipment software update	76
SE3 - Security of access to services	77
SE3.1 Securing access to applications	77
SE3.2 Prevention and management of risks	78
SE4 - Data Protection	79
SE4.1 Compliance with the General Data Protection Regulation	79
Responsible management.....	81
Scale of points per requirement	82
MA1 - Project governance	84
MA1.1 SMART information in the contractual documents	84
MA1.2 Administration of the Smart Network	85
MA1.3 Acceptance testing of the Smart Network	86
MA2 - Property ownership	89
MA2.1 Ownership of the infrastructure of the Smart Network	89
MA2.2 Ownership of data	89
MA3 - Framework for services contracting.....	90
MA3.1 Service level agreements (SLA) with suppliers	90
MA4 - Environmental qualities.....	91
MA4.1 Determination of the electromagnetic field and provisions made.....	91
MA4.2 Supply of PEP environmental sheets	92
MA5 - Management system	93
MA5.1 Project management.....	93
MA5.2 Involvement of stakeholders	95
Services.....	96
Scale of points per requirement	97
SE1 - Energy services	98
SE1.1 Installation of an energy monitoring platform	98
Glossary	100



Introduction

Context and objectives

Digital technology at the service of the building and its occupants

Within one generation, digital technology has become the central driver of our economic development and a powerful agent for change in our daily lives. It interacts with the objects that surround us, the places where we live and work and on our way of life in general. New services are appearing, new connected objects are invented and new patterns of use are emerging, each offering an ever-wider choice, stimulating our ability to interact with the world that surrounds us.

This phenomenon affects the building sector, which must meet new challenges related to the digital transition:

- ensure an optimal Internet connection;
- respond to requests from users;
- ensure the security of networks and the protection of personal data;
- increase the sustainability of installations;
- use the most appropriate digital tools for building and operation (e.g.: digital model,...);
- combine the digital revolution with sustainable development;
- promote the integration of buildings into the digital and sustainable city...

The digital transition implies a new way of designing, constructing and operating the building. The human aspect must also remain at the centre of our concerns, as the purpose of the building is to provide users with greater comfort, more social connections and greater efficiency at work, to simplify their daily lives, while preserving the environment.

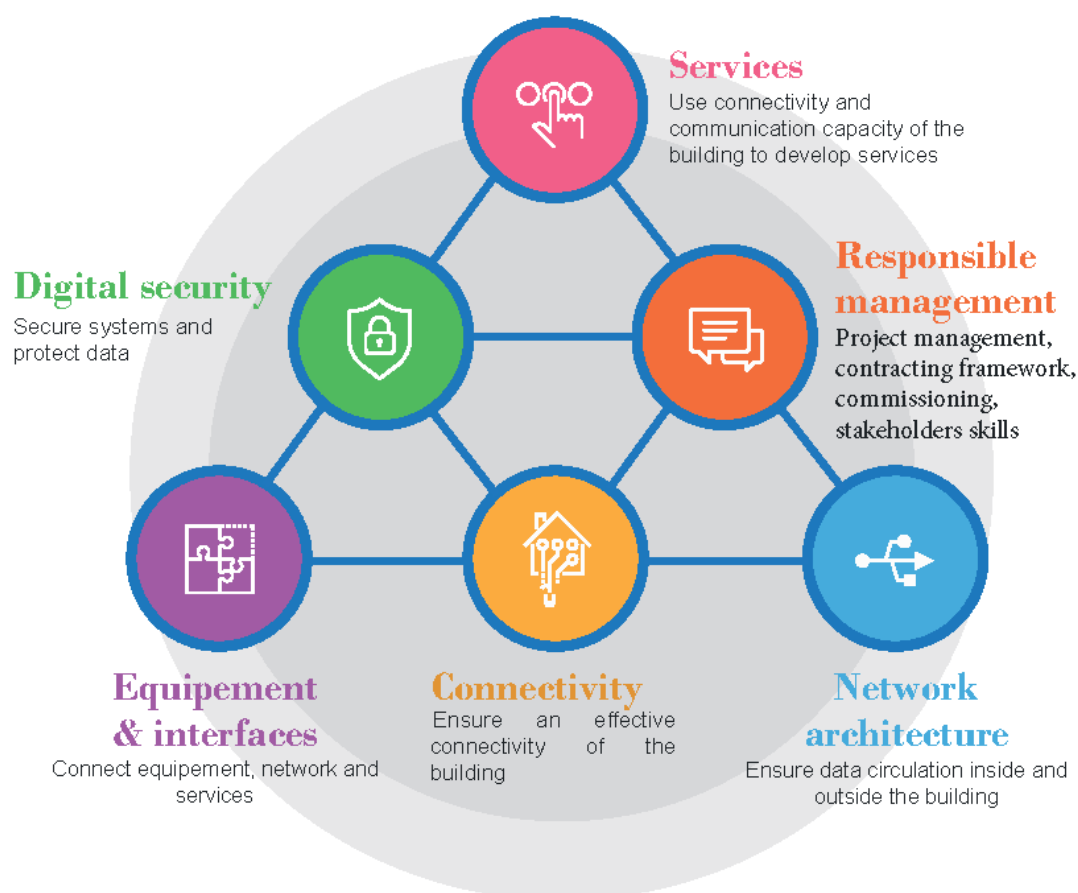


R2S label: technical resources for a high-performing and sustainable architecture

The R2S-Ready2Services label is built around a scheme that describes the technical and organisational resources to put in place to support the digital transition of the building. These resources are intended to ensure high-performing communication with a reliable infrastructure for connectivity and to organise the interoperability of systems that were previously isolated from each other by integrating common protocols (IP – Internet Protocol). Thanks to this interoperability, the building, because it is no longer fixed, fulfils current needs or expectations, while being capable of satisfying the requirements of the future. These conditions enable the building to become a real services platform, comprehensive and scalable over time, also increasing its usage value.

The Ready2Services label is intended to prepare the connected and communicating building to receive a full range of digital services, thus making it adaptable, pleasant to live in and able to interact with its environment, to eventually form part of an approach towards the sustainable and intelligent city.

The R2S scheme describes the technical and organisational resources to be put in place so that a building can respond to the challenges of the transformation of usage patterns by digital technology. These issues are grouped in the six themes visible below:





Main principles and definition framework of the Ready2Services label

The key principles of the Ready2Services approach:

The R2S-Ready2Services approach has **three independent layers**. They offer buildings great flexibility and scalability by disassociating the application layer (the services), the communication layer (the building's network infrastructure) and the material ecosystems layer (equipments). The R2S model sets the rule of interchangeability of each layer, without modifying the other two, so that a service does not impose a hardware ecosystem or a dedicated network infrastructure, and reciprocally. This way, these three layers communicate, interact and exchange data which converge via the building's Smart Network (see the glossary at the end of this document).

The R2S-Ready2Services label favours technical means intended to ensure efficient communication and the **interoperability of systems**, integrating common protocols (IP – Internet Protocol –) and services having open APIs (programming interfaces).

Openness of data and security: the interfaces chosen within the connected building enable control functions and information to be accessible inside and outside the building. Digital security is the corollary of this principle of openness: protection of data, resilience and IT security.

The framework of definition includes six themes, included in the present scheme:

► 3 themes related to technical principles:

Connectivity: ensure high-performance connectivity of the building via an optimal connection to communication networks.

Network architecture: ensure the circulation of data inside and outside the building by improving the characteristics of the building's networks.

Equipment and interfaces: relate equipment, the network and services through their interoperability.

► 2 themes related to governance

Digital security: secure systems and interfaces and set up a system for protecting personal data.

Responsible management: optimise the management of the project and commissioning, set up a framework for contracting and work with competent players.

► 1 theme related to occupants and to the building:

Services: use the building's capacity for connectivity and communication to develop services.

Scope of application

Perimeter of labelling

Spatial and activity perimeter

The approach applies to all non-residential buildings (offices, retail, education, hotels,...). For other specific activities such as logistics, laboratory, research activities, health establishments, sporting facilities,... we provide advice to evaluate the feasibility of the request.

Labelling is possible for a building or an estate of buildings.

The request for labelling is done for a given layout, the layout corresponding to one or more buildings or a part of a building. For a building having several activities (example: offices and retail outlets at the bottom of the building), you have the option to evaluate the entire building or separate the activities of the building by carrying out different evaluations.

Technical perimeter

The Ready2Services scheme requires a "Smart Network" as a prerequisite. It is a unifying network within the building using the Internet Protocol and the Ethernet standard (for more details, see the definition below). A prior condition for R2S labelling therefore consists of defining the perimeter of the Smart Network. Definition of this perimeter is left free to the originator of the process.

Thus, the requirements related to the Smart Network only concern the network and the perimeter as defined by the originator of the process. Likewise, "active equipment" corresponds only to equipment that is connected to the Smart Network. Other active equipment connected to other networks need not prove levels of requirements fixed in the scheme.

Definition: The "Smart Network" is the unifying network of an R2S building, service-oriented (SOA) and using the protocol IP. It is secured and exclusively uses the Ethernet standard on the local network and the Internet standard from the exterior of the building. The hardware ecosystems, whatever their protocol, communicate on the Smart Network using APIs or web services exposed on the Smart Network and on the World Wide Web.

Commitment to a labelling process

The process of R2S-Ready2Services labelling can be carried out on construction projects that are new, under renovation or in operation.

For buildings under construction and renovation, entry into labelling is done from the design or execution stage of a project. For projects entering labelling in the design stage, the Project Owner undertakes to go as far as the execution stage. A documentary check is planned in the design stage and an on-site check in the execution stage.

For buildings in operation, it is for the applicant for the label to choose the rate of its labelling, from 1 to 3 years, but a period of 3 years is recommended for greater efficiency. A check on site is planned during the first year (unless the project is labelled in construction, in which case the on-site check is postponed) for 1 or 3 years of follow-up. In the case of follow-up over 3 years, a documentary analysis is done between 12 and 24 months after the admission check. It is timed as chosen by the project owner.



In concrete terms, the stages may be defined as follows:

- Entry into the Design stage: after the finalisation of the tender document. The applicant undertakes to go as far as the execution stage.
- Entry into the Execution stage: before expiration of the completion guarantee.
- Entry into the Operation stage: after the building's commissioning. The interventions occur every year. The contract is tacitly renewed each year.

Before each check, a limited number of preparatory modes of evidence must be sent to the auditor. The list of documents to be sent is detailed in the document present for each requirement according to the stage in which the building is located and the level of performance targeted.







Structure and scoring system

Structure of the scheme

The Ready2Services scheme is composed of six themes:

- Connectivity
- Network architecture
- Equipment and interfaces
- Digital security
- Responsible management
- Services

These themes include the following sub- topics:

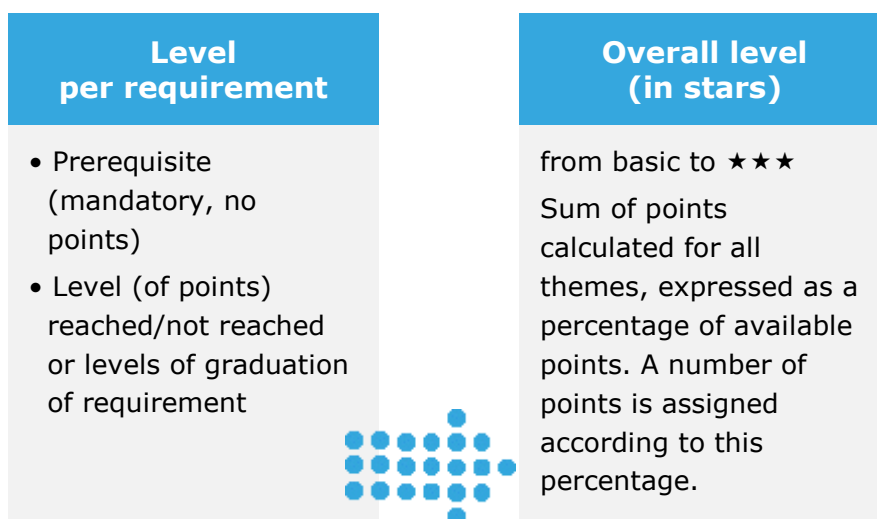
 Connectivity	 Network architecture	 Equipment and interfaces	 Digital security	 Responsible management	 Services
Connection to the building's external networks	Smart network and occupants' network	Communication interfaces	Security of networks and building systems	Project governance	Energy services
Connectivity to land line networks	Continuity and functional protection of the Smart networks	Openness of systems	Network security procedures	Property ownership	
Connectivity to wireless networks	Management of the Smart network	Access to data and services	Security of access to services	Framework for contracting services	
Usability and scalability of cabling			Protection of data	Environmental qualities	
Redundancy and security of cabling				Management system	

Evaluation system

A scoring system was created so that each player can measure, compare and evaluate the performances of their building. It may be used to control performance or to report internally or to clients and decision-makers. These measurements are automatically calculated on Cerway's digital platform: ISIA (see below).

The Ready2Services scheme is broken down into six themes, themselves divided into sub-topics which represent the major concerns associated with each challenge involving connected and communicating buildings, then into requirements.

The scoring system for the building consists of assigning a number of points for each requirement. The number of points per theme is then calculated via ISIA and an overall performance level for the project is deduced from this, going from "base" level to 3-star level.



The distribution of points

For each level, it is necessary to obtain a percentage of points defined in the table below:

Level	Base	★	★★	★★★
% of number of points to be obtained to reach the level	>20%	40%	60%	80%

To be labelled, one must be at least at the Base level, meaning having fulfilled all prerequisites, and obtain at least 20% of points.

The number of points per requirement is specified in the details of requirements in the present document.

In the Ready2Services label, it is possible to obtain bonus points. They constitute points which are added to the final score and are intended to evaluate projects that include – or have included – the network of users in the construction tenders. These bonus points are optional: the non-achievement of the requirements concerned does not prevent obtaining 100% points in the ready2Services label.

A display in the form of the logo for the R2S label accompanied by the number of stars obtained can be used to promote your project internally and externally.

Identification

The following criteria are to be completed for your evaluation in the ISIA tool. These criteria can quickly and simply configure the contextual display of the requirements that correspond to your project.

Requirements	List of ISIA choices	Comments
ID1.1 Type of project	New construction Renovation Operation	
ID1.2 Stage at the moment of evaluation	Design Execution	<i>Requirement dependent upon projects under new construction or renovation</i>
ID1.3 Main activity of the sub-object	Office building Education Retail Hotels Shows Culture	
ID1.4 Surface (m² GFA)	(entry field)	
ID1.5 Use of a digital model (BIM)	Yes / No	

As a reminder, an object designates the element or elements that constitute the project.

••• ► A building = 1 object, except in the case of buildings right next to each other.

A sub-object designates the sector and the activity of the labelled object on which the project owner wishes to communicate. The requirements according to which the evaluation is carried out depend on the sub-object. Therefore an object (building) may, for example, have several sub-objects (offices and shops at the foot of the building).

Key stages

1. Contracting: dispatch of the application form accompanied by substantiating documentation; after studying the documents sent, Cerway issues and accepts the contract.

3. Verification: an independent auditor analyses the project. A complete report is then sent to the applicant for the label with the findings of the intervention: strong points, sensitive points, ways for improvement, non-compliances. This enables the applicant to take the necessary corrective actions in case of non-compliances. Constructive exchanges between Cerway and the applicant enable the evaluation of the project to be validated and qualified with a performance threshold from Base level to 3 star level.

ISIA, the online platform dedicated to R2S-Ready2Services labelling

ISIA makes it possible to calculate the level of performance achieved as the project progresses, to publish personalised reports, and to exchange with the various stakeholders (technical questions or questions about the labelling procedure, etc.).





Details of the requirements



connectivity

CO1 - Connection to the building's external networks

CO2 - Connectivity to land line networks

CO3 - Connectivity to wireless networks

CO4 - Usability and scalability of the cabling

CO5 - Redundancy and security of the cabling



Connectivity

This theme aims to ensure high-performance connectivity for the building, which is a basic foundation necessary for setting up digital services. A labelled building is connected to communication networks, whether they are internal or external, land line or wireless (Wi-Fi, GSM, 3G, 4G...), in the common and private areas.

This connection can route any type of link in accordance with international public standards. Furthermore, the cabling for a labelled building is characterised by its adaptability and scalability. Indeed, it is

possible to associate or disassociate cabling without renovation, to adapt to new operating requirements or the integration of new communicating systems.

Lastly, the theme sets out to ensure the reliability of connectivity with redundancy of the connection for the building and the active equipment of the Smart Network, which can provide continuity of service in case of a failure. Finally, a protection system is required to ensure the security of the Smart Network against any abusive actions.

Scale of points per requirement

Title of the requirement	Level	Points
CO1 - Connection to the building's external networks		
CO1.1 Building prepared for connection to any type of external land line	Prerequisites Achieved / not achieved	/
	Level 1 Capacity for connection to the networks of at least 4 operators.	1
	Level 2 (bonus) Pre-arrangements for the internal routing of external operator links	1
CO1.2 Redundancy of the building's connection to all types of external land line	Level 1 Existence of a second operator room or space.	1
	Level 2 Creation of a second structure under roads or utility networks	2
	Level 3 (bonus) Pre-arrangements for the internal redundant routing of external operator links	3



Title of the requirement	Level	Points
CO2 - Connectivity to land line networks		
CO2.1 Cabling the building's general communication services	Prerequisites Achieved / not achieved	/
	Level 1 Completion of Smart Network cabling.	1
CO2.2 Preparation of cabling for the property units / activity areas of the building	Level 1 Installation of pathways.	1
	Level 2 Implementation of the cabling.	2
	Level 3 (bonus) Implementation of modular pre-cabling.	2
CO3 - Connectivity to wireless networks		
CO3.1 Nature and quality of the wireless networks	Level 1 Supply of a coverage study.	1
	Level 2 GSM network in the common parts.	2
	Level 2 bis Wi-Fi network in the common parts.	1
	Level 2 ter Wi-Fi network in the private parts.	1
CO4 - Usability and scalability of the cabling		
CO4.1 Adaptability of the cabling distribution	Level 1 Extension capacity for adding new IT/communication sockets.	1
	Level 1 bis Distribution of terminals and sockets by pre-terminated cables or extensions.	1
CO5 - Redundancy and security of the cabling		
CO5.1 Redundancy capacity of the building's cabling	Level 1 Presence of two cable distribution routes.	1
	Level 2 Presence of two general distribution rooms or spaces.	2
	Level 3 Redundancy of links serving the connection nodes of the Smart Network.	3



Title of the requirement	Level	Points
C05.2 Electrical power supply to the infrastructure	Level 1 Uninterruptible power supply to the central active equipment.	1
	Level 2 Stabilised power supply to the active equipment.	2
	Level 3 Redundant power supply to the active equipment.	3
	Level 4 Redundant electrical power supply.	4
C05.3 Access control and protection of infrastructure	Level 1 Protection of connection nodes without traceability.	1
	Level 2 Protection of connection nodes with traceability.	2



CO1 - Connection to the building's external networks

CO1.1 Building prepared for connection to any type of external land line

• • • ► List of ISIA choices:

- Capacity for connection to the networks of at least 2 operators
- Capacity for connection to the networks of at least 4 operators
- Preparation of internal routing of external operator links

The building is prepared to be connected to the external networks of operators and to enable the distribution of any type of link operated towards its general distribution room.

Note: A level of this requirement includes bonus points. They constitute points which are added to the final score and are intended to evaluate projects that include – or have included – the network of users in the construction contract. These bonus points are optional: the non-achievement of the requirements concerned does not prevent obtaining 100% points in the ready2Services label.

✚ Prerequisites: Capacity for connection to the networks of at least **2 operators**

This requirement aims to guarantee that the building is connected to the land lines of *up to 2 telecoms operators*, each having its dedicated space.

A cable network structure must be created up to the limit of the public domain, enabling the building to be connected through conduits to the networks of at least 2 operators.

From the public domain, this cable network structure must be extended by:

- Equivalent routing to the operator room or space,
- AND equivalent routing to the general distribution room.

The operator rooms or spaces and general distributor room have a floor surface of 8 m² or more, with 2.4 m minimum width.

MODES OF EVIDENCE

Levels of Prerequisites and Level 1:

- **Design:** Extract from the specifications and required documents showing the integration of requirements in the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.

(continued on following page)



• Level 1: Capacity for connection to the networks of at least **4 operators**

This requirement aims to guarantee that the building is connected to the land lines of *up to 4 telecoms operators*, each having its dedicated space.

See the detailed description above in Prerequisites.

• Level 2 (bonus): Preparation of internal routing of external operator links

This requirement concerns the preparation of the building to route external links (high and low bit-rate depending on local availability) towards the cables for the general services and the activity areas of the premises.

The requirement covers:

- compliance with the Prerequisite level,
- + the installation of 2 x 19 inch containers in the operator and general distribution spaces or rooms of the building.

The two 19 inch containers in this requirement are dedicated to the interconnection links of the operator rooms. These interconnection links are composed of twisted wire pairs and/or optical fibre links.

If twisted wire pairs are present, they must include at least 32 pairs for General Services and 8 pairs per property unit (or for all of the activity areas). The containers may also be constituted (as well as the twisted-wire pair links or as an alternative to them) by optical fibre links with a minimum of 6 strands for general services and each private property unit, or for all of the activity areas (according to the local availability of switched telephone networks and optical fibre networks of operators).

- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.

MODES OF EVIDENCE

Level 2 (bonus):

- **Design:** Extract from the specifications and required documents showing the inclusion of requirements in the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Document identical to the prerequisites and level 1, providing that level 2 has been validated during completion.



CO1.2 Redundancy of the building's connection to all types of external land line

• • • ► List of ISIA choices:

- Existence of a second operator room or space
- Creation of a second cabling network structure
- Preparation of redundant internal routing of external operator links

The building makes the necessary provisions to ensure redundant connections to the operator networks. It is provided with at least two operator rooms or spaces enabling connection to at least two separate operators.

Note: A level of this requirement includes bonus points. They constitute points which are added to the final score and are intended to evaluate projects that include – or have included – the network of users in the construction contract. These bonus points are optional: the non-achievement of the requirements concerned does not prevent obtaining 100% points in the ready2Services label.

• • Level 1: Existence of a second operator room or space

This is to make it possible to continue service in case of the unavailability of one of the two operator rooms.

A second room or operator space exists in the building; it has a floor area of at least 8 m² and at least 2.4 m in width.

• • Level 2: Creation of a second road/utility network structure

This is to make it possible to continue services in case of damage to one of the cabling network structures connecting the building to the external networks.

The requirement is to comply with the preceding level 1 and to also create a second cabling network structure at least 8 m away from the first, as far as the limit of the public domain, enabling the connection through conduits of the building to the networks of at least two operators.

MODES OF EVIDENCE

Levels 1 and 2:

- **Design:** Extract from the specifications or plans showing the inclusion of requirements in the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.



• Level 3 (bonus): Preparation of redundant internal routing of external operator links

The requirement demands compliance with the aforementioned level 1 and installation of a 19 inches container in the second operator space or room, dedicated to the links that connect with the first operator space or room and the general distributors.

The two 19 inches containers in this requirement are dedicated to the interconnection links of the operator rooms. These interconnection links are composed of twisted wire pairs and/or optical fibre links.

If twisted wire pairs are present, they must include at least 32 pairs for General Services and 8 pairs per property unit (or for all of the activity areas). The containers may also be constituted (as well as the twisted-wire pair links or as an alternative to them) by optical fibre links with a minimum of 6 strands for general services and each private property unit, or for all of the activity areas (according to the local availability of switched telephone networks and optical fibre networks of operators).

MODES OF EVIDENCE

Levels 3:

- **Design and Execution:** same as levels 1 and 2.
- **Operation:** Document identical to levels 1 and 2, providing that level 3 has been validated in completion.



CO2 - Connectivity to land line networks

CO2.1 Cabling the building's general communication services

• • • ► List of ISIA choices:

- Completion of cabling for the General Services Smart Network
- Completion of Smart Network cabling

The building is provided with cabling for the Smart Network grouping the links and connections to all of the communicating systems of general services.

• Prerequisites: Completion of cabling for the General Services Smart Network

To fulfil the requirement, the building must be fitted with single unifying cabling, grouping the links and connections of all of the communicating systems from the general services to the building's Smart Network.

This leads to:

- The installation of a 19 inch container in the access-controlled general distributor room, and cable paths and supports for the Smart Network.
- The installation of cabling supporting the Ethernet-IP links of the Smart Network.

• Level 1: Completion of Smart Network cabling

At level 1, the prerequisites must be fulfilled and standardised cabling must be completed for the Smart Network. This cabling can route low bit-rate analogue or digital links to any location in the building, from an operator network or a local source.

MODES OF EVIDENCE

All levels:

- **Design:** Extract from the specifications or plans showing the inclusion of requirements in the design file.
Examples: Special Technical Specifications, specifying the cabling system, the cabling diagram and the installation plan for the utility ducts.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.



CO2.2 Preparation of cabling for the property units / activity areas of the building

- • • ► List of ISIA choices:
 - Installation of pathways
 - Installation of the cabling
 - Installation of modular pre-cabling

The building is prepared to receive the cabling or network equipment, bringing together the connections for the private communicating systems of the various activity areas or property units.

In the Ready2Services label, it is possible to obtain bonus points. They constitute points which are added to the final score and are intended to evaluate projects that include – or have included – the network of users in the construction contract. These bonus points are optional: the non-achievement of the requirements concerned does not prevent obtaining 100% points in the ready2Services label.

••• Level 1: Installation of pathways

The challenge of this requirement is to prepare the building to receive the cables and equipment of the networks and systems of future users.

Pathways are provided to support the operator cabling of each property unit. This is the case from each property unit as far as the operator and general distributor rooms.

••• Level 2: Installation of the cabling

The challenge of this requirement is the preparation of the building's cabling to route any type of link towards its private units or its activity areas.

In this regard, the requirement is

- compliance with the aforementioned level 1;
- + the implementation of cabling between, firstly, the operator premises and the general distribution premises, and secondly each property unit, with a minimum of 6 twisted copper pairs or 6 strands of optical fibre. The cabling put in place is pre-terminated, has cable slack of 5 m on the side of the operator room (the cable ends in a 19 inch container and general distribution), and 15 m in the property unit or activity area.

MODES OF EVIDENCE

Levels 1 and 2:

- **Design:** Extract from the specifications or plans showing the inclusion of requirements in the design file.
Examples: Special Technical Specifications, specifying the cabling system, the cabling diagram and the installation plan for the utility ducts.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.



🔧 Level 3 (bonus): Installation of modular pre-cabling

The private areas are pre-fitted with movable, modular and scalable cabling, "Cabling as a service": it enables quick installation of the future user or occupant; it makes possible the management, by the future user/occupant or the facility manager, of a modular connection routing service.

This level 3 of the requirement covers:

- compliance with the two previous levels;
- + the implementation of modular pre-cabling with pre-connected cabling components. This modular pre-cabling consists of local connection nodes spread within the private areas and distributing sockets by cables and/or removable extensions, enabling the connection of IT/communication terminals.

MODES OF EVIDENCE

Levels 3:

- **Design and Execution:** same as levels 1 and 2.
- **Operation:** Document identical to levels 1 and 2, providing that level 3 has been validated in Execution.





CO3 - Connectivity to wireless networks

CO3.1 Nature and quality of the wireless networks

- • • ► ISIA multiple choice list:
 - Supply of a GSM coverage study
 - GSM in the common parts
 - Wi-Fi network in the common parts
 - Wi-Fi network in the private parts

The building has adequate coverage inside its various spaces for the main radio networks (GSM, Wi-Fi...).

The quality of coverage of wireless networks (examples: reception power, multiplexing, simultaneous communication,...) must be defined by the project owner coherently with the services that must be provided by these networks.

The Wi-Fi networks must have a mechanism enabling a device to change access points without losing its connectivity and therefore without interruption of services during movement (handover or roaming mechanism).

By default, the common and private parts where the requirement levels apply may be defined as follows:

- Common parts: The spaces of the building likely to be frequented by all occupants of the building, visitors, service providers in charge of safety/security, maintenance and the operation of the systems and services of the building and the public, where applicable.
- Private parts: Spaces of the building frequented only by the occupants for whom they are intended for their activities and by visitors authorised by these occupants.

To put the requirement into context, the definition specifies that the common and private parts may be left to the choice of the project owner, who must thus define the zones considered as common and private parts. It must be able to justify the choice of zones with arguments (use of rooms and the services proposed within them, public frequenting defined zones,...).



Level 1: Supply of a coverage study

The challenge of this requirement is to give future occupants visibility concerning the quality of access, within the building, to the main radio networks (GSM, Wi-Fi).

A study on the coverage of public GSM networks under 2G/Edge/3G/4G should therefore be provided according to their local availability.

Level 2: GSM in the common parts

This level of requirement aims to provide a guarantee of access, in all interior spaces of the building, to the GSM networks available from the operators.

This level of requirement covers:

- compliance with level 1;
- + the equipment of the common parts with a GSM network.

Level 2 bis: Wi-Fi network in the common parts

The challenge of this level of requirement is the availability of Wi-Fi coverage in the common spaces of the building.

This level of requirement covers:

- compliance with level 1;
- + equipment of the common parts with a single Wi-Fi network (roaming).

Level 2 ter: Wi-Fi network in the private parts

The challenge of this level of requirement is the availability of Wi-Fi coverage in the private spaces of the building.

This level of requirement covers:

- compliance with level 1;
- + equipment of the private parts with a single Wi-Fi network (roaming).

MODES OF EVIDENCE

All levels:

- **Design:** Extract from the specifications showing the inclusion of requirements in the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.

Example of modes of evidence: Readings of levels of GSM and/or Wi-Fi power according to the floors inspected, technical information sheets for products.



CO4 - Usability and scalability of the cabling

CO 4.1 Adaptability of the cabling distribution

• • • ► ISIA multiple choice list:

- Extension capacity for adding new IT/communication sockets
- Distribution of terminals and sockets by pre-terminated cables or extensions

The cabling for the building allows easy addition, deletion or modification of the density or location of the points of connection of communicating equipment.

This concerns promoting the ease of adaptation of the cabling. This adaptability is necessary for various scenarios:

- for the integration of additional communicating systems or equipment;
- for the redistribution and/or revision of the density of sockets in the private spaces, according to redevelopments made and the evolution of requirements for connectivity of the occupants of the building.

Note: This requirement applies to the cabling of general services and extends to the cabling in the private spaces if it is provided when the building is delivered.

✚ Level 1: Extension capacity for adding new IT/communication sockets

Caution: this level of requirement applies only to the Design and Execution stages of the project.

It concerns the capacity for adding sockets in the building.

It requires a minimum extension capacity of 30% for subsequent addition of IT/communication terminals on the Smart Network from a utility room or cabinet.

MODES OF EVIDENCE

Level 1:

- **Design:** Extract from the specifications showing the inclusion of requirements in the design file.
Example of modes of evidence: Special Technical Specifications, for the cabling system, the cabling diagram and the installation plan for the utility ducts.
- **Execution:**
Construction documents for checking the actual extension capacity.
(Same examples of modes of evidence as above in the design stage).



❖ Level 1 bis: Distribution of terminals and sockets by pre-terminated cables or extensions

This level of requirement concerns the easy redistribution of sockets in the building.

It requires the terminals and sockets to be distributed using pre-terminated cables or extensions, connected to a connection unit and/or active equipment of the Smart Network. This unit must be placed near to the terminals. The links may or may not be distributed from a utility room or cabinet on the floor.

MODES OF EVIDENCE

Level 1 bis:

- **Design and Execution:** same as Level 1
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.



CO5 - Redundancy and security of the cabling

CO5.1 Redundancy capacity of the building's cabling

- • • ► List of ISIA choices:
 - Presence of two cable distribution routes
 - Presence of two general distribution rooms or spaces
 - Redundancy of links serving the connection nodes of the Smart Network

The infrastructure of the building's cabling system is redundant.

Redundant cabling does not have any Single Point of Failure (SPOF) between the connection nodes of the sockets and the general distributor receiving the central network equipment. All of the links serving equipment of the Smart Network and connecting the Ethernet-IP terminals are duplicated, laid out on separate routes and attached to two general distributors. These general distributors are connected between each other and with the operator spaces.

• • • ► Level 1: Presence of two cable distribution routes

The aim of this requirement is to evaluate the preparation of the building to receive redundant cabling.

The building has two vertical utility ducts, spaced at least 8 m apart (or 2 m with a fire break). These ducts are fitted with pathways dedicated to IT/communication cabling, thus providing two separate routes for distributing to each of the floors of the building from the operator and general distribution spaces.

• • • ► Level 2: Presence of two general distribution rooms or spaces

This level of requirement is intended to check that the building is prepared to enable redundancy for its central equipment.

It requires:

- compliance with the aforementioned level 1;
- the presence in the building of a second general distribution room or space having identical characteristics to the first. It is spaced at least 8 m from it (2 m with a fire break) and has a

MODES OF EVIDENCE

All levels:

- **Design:** Extract from the specifications and plans showing the integration of requirements into the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.

Examples of modes of evidence valid for the three stages: Special Technical Specifications, for the cabling system, the cabling diagram and the installation plan for the utility ducts.



different vertical descent. Pathways of a capacity adapted to the quantity of cables to be installed interconnect this second room:

- ✓ to the cable distribution pathways in the building,
- ✓ to the 1st general distributor room,
- ✓ and to the operator rooms or spaces.

Level 3: Redundancy of links serving the connection nodes of the Smart Network

This requirement level is intended to check that the Smart Network is made reliable by hardware redundancy of the access network as close as possible to the terminal equipment.

It requires:

- compliance with the two previous levels;
- + redundancy of the links between the general distributors and the sub-distribution points.



C05.2 Electrical power supply to the infrastructure

• • • ► List of ISIA choices:

- Uninterruptible power supply to the central active equipment
- Stabilised power supply to the active equipment
- Redundant power supply to the active equipment
- Redundant electrical power supply

The cabling of the general services of the building's Smart Network has electrical distribution systems guaranteeing the stability and security of the electrical power for the network connection nodes.

• Level 1: Uninterruptible power supply to the central active equipment

The aim of this level of requirement is to guarantee availability of current for which the voltage and frequency are regulated, in order to best guarantee the functional continuity of the central active equipment of the Smart Network and local servers. It also concerns giving the building sufficient autonomy to enable this equipment to be shut down according to the procedure recommended by the manufacturers.

This level of requirement needs an uninterruptible power supply to the central active equipment of the Smart Network (network cores, routing, firewall and interface equipment with the telecommunication operators' networks) and the local servers that are attached to them. This equipment shuts down automatically in case of a prolonged cut-off of the main source and the autonomy of the uninterruptible power supply is sufficient for this process to proceed.

MODES OF EVIDENCE

Level 1:

- **Design:** Extract of the specifications and diagrams (smart network and high-current wiring) demonstrating the integration of the requirements into the design file.
- **Execution:** Diagrams (Smart Network and high-current wiring) AND functional analysis of automatic shutdown AND power balance to justify autonomy.
- **Operation:** Certificate of current guarantee for consumable equipment (example: electrical batteries) OR test report for this equipment. Up-to-date diagram of the Smart Network and high-current wiring.



Level 2: Stabilised power supply to the active equipment

The aim of this requirement is to have stabilised power for all of the active equipment of the Smart Network.

It requires:

- compliance with level 1 of the requirement;
- + stabilised power supply to the points of sub-distribution of the active equipment of the Smart Network, including for the wireless networks that are attached to it.

Level 3: Redundant power supply to the active equipment

This level of requirement concerns the guarantee on continuity of services of active equipment of the Smart Network, in case of the failure of a power circuit.

It requires:

- compliance with the two previous levels of the requirement;
- + the presence of a redundant electrical power supply with no single point of failure for the active equipment of the Smart Network (excluding wireless networks) and the servers that are attached to them.

Level 4: Redundant electrical power supply

This last level of the requirement is intended to guarantee continuity of the services of the Smart Network in case of an electrical power cut of indeterminate duration.

It requires:

- compliance with the three previous levels of the requirement;
- + the presence of two normal sources of electrical power to supply the Smart Network (examples: public network + permanent-production renewable energy, or electricity generator, or double branch on the public distribution network).

MODES OF EVIDENCE

Level 2:

- **Design:** Same as level 1.
- **Execution:** Additional high-current wiring diagram for the sub-distribution points.
- **Operation:** Up-to-date diagram of the Smart Network and high-current wiring.

MODES OF EVIDENCE

Level 3:

- **Design:** Same as level 1.
- **Execution:** High-current wiring diagrams and technical information sheets to justify the dual power supply to active equipment of the Smart Network.
- **Operation:** Same as level 2.

MODES OF EVIDENCE

Level 4:

- **Design:** Same as level 1.
- **Execution:** High-current wiring diagram AND functional analysis to justify the switchover mode between the two sources.
- **Operation:** Same as level 2.



C05.3 Access control and protection of infrastructure

• • • ► List of ISIA choices:

- Protection of connection nodes without traceability
- Protection of connection nodes with traceability

A protection system must be set up to secure the infrastructure of the Smart Network of the building against any unauthorised access.

This requires a description of the conditions for access to the utility rooms (operators, general distribution, service,...) and points of sub-distribution of the Smart Network.

Access to these premises or points of sub-distribution must be accessible only to authorised personnel.

• Level 1: Protection of connection nodes without traceability

This level of requirement concerns the protection of access to cables in utility ducts and to electronic IT/communication equipment of the Smart Network.

It requires protection of access to sub-distribution points. This security can be provided by locking a utility room or cabinet using a means without traceability (key, code,...).

• Level 2: Protection of connection nodes with traceability

This level of requirement concerns the protection and traceability of accesses to cabling and equipment of the Smart Network.

It requires:

- compliance with level 1 of the requirement;
- traceability of access to the cabling and equipment of the Smart Network (electronic cylinder lock, access control badge,...).

MODES OF EVIDENCE

All levels:

- **Design:** Extract from the specifications and plans showing the integration of requirements into the design file.
Example of modes of evidence: Special Technical Specifications, for the cabling system, the cabling diagram and the installation plan for the utility ducts.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements



Network rchitecture

RE1 - Smart Network and occupants' networks

RE2 - Continuity and functional protection of the Smart Network

RE3 - Management of the Smart Network





Network architecture

The challenge of this theme is to ensure the circulation of the 4th utility fluid of the building, namely data, which constitutes its backbone. The Ready2Services scheme requires a Smart Network as a prerequisite. It is a unifying network of the building, using the Internet Protocol and the Ethernet standard.

A prior condition for R2S labelling therefore consists of defining the perimeter of the Smart Network. Definition of this perimeter is left free to the originator of the process. Thus, the requirements related to the Smart

Network only concern the network and the perimeter as defined by the originator of the process. Likewise, "active equipment" correspond only to equipment that is connected to the Smart Network. Other active equipment connected to other networks need not prove achievement of performance levels fixed in the scheme.

The labelled building will be evaluated on the characteristics of active equipment and the administration, management and functional protection of the Smart Network.

Scale of points per requirement

Title of the requirement	Level	Points
RE1 - Smart Network and occupant's networks		
RE1.1 Smart Network dedicated to the general services of the building	Prerequisites: Achieved / Not achieved	/
RE1.2 Networks dedicated to the communication services of occupants	Level 1 (bonus points): Installation of network equipment containers	1
	Level 2 (bonus points): Installation of switches	2
	Level 3 (bonus points): Future users' networks activated and administered	3





Title of the requirement	Level	Points
RE1.3 Power supply to the communication services of occupants	Level 1: Protective measures for PoE	1
	Level 2: PoE ports on the access switches	2
	Level 3: Extension capacity of switches	4
	Level 4: Activation of delivery of controllable PoE	5
RE1.4 Support of the IPv6 protocol	Achieved / Not achieved	3
RE2 - Continuity and functional protection of the Smart Network		
RE2.1 Resilience capacity of the Building's Smart Network	Level 1: Dual connection of network access equipment	3
	Level 2: Resilience of the redundancy mechanism	5
RE2.2 Detection of malfunctions and protection of the Smart Network	Unique level (achieved / not achieved): Smart Network protected against network functional malfunctions of the equipment connected to it	3
RE3 - Management of the Smart Network		
RE3.1 Administration of networks and their equipment	Level 1: Centralised administration platform for active equipment of the Smart Network	2
	Level 2: Support to version 3 of the SNMP protocol	3
	Level 3: Administration platform for all equipment of the Smart Network	4



Title of the requirement	Level	Points
RE3.2 Prioritisation and continuity of service of the networks	Level 1: Quality of Service (QoS) function available and activated	2
	Level 2: Contractual commitment for a Guaranteed Resolution Time of 8 hours	3
	Level 3: Contractual commitment for a Guaranteed Resolution Time of 4 hours	4
	Level 4: Contractual commitment to service continuity	5
RE3.3 Common services of the Smart Network	Achieved / Not achieved	3



RE1 - Smart Network and occupants' networks

RE1.1 Smart Network dedicated to the general services of the building

• • • ► List of ISIA choices:

- Achieved / Not achieved

The IT and communication systems of the general services of the building and of its users must be connected to a unifying Ethernet-IP network hereafter called the "Smart Network".

An electronic network dedicated to the general services systems must exist upon delivery of the building. This electronic network constitutes the unifying network for transporting information for the communicating systems of the building.

It must be compliant with the international TCP/IP and Ethernet standards IEEE 802.1xx, 802.3xx and 802.11xx if a Wi-Fi network is implemented.

It must connect equipment in the communicating systems of the general services (other than the Fire Safety System), either natively using Ethernet or Wi-Fi, or via a cable or radio protocol gateway, to make them accessible from the Internet or an Intranet.

The network must manage the routing function in a secure manner and notably inter-VLAN routing. This network may be physically common with those of the occupants; in this case, VLAN must also be dedicated to their communicating systems. The Ethernet packets of the network must not be encapsulated in another protocol.

This unique requirement, with the status of a prerequisite, requires the sharing of network equipment by all communicating systems of the general services.

This prerequisite is intended to promote interoperability and access to the services by defining a Smart Network compliant with international public standards.

This prerequisite requires the existence of a Smart Network having at least routing functions (level 3) and switches of at least of level 2.

MODES OF EVIDENCE

Prerequisites

- **Design:** Extract from the specifications describing the Smart Network with its architecture and routing and level 2 switching functions OR diagram specifying this same information. Examples: Special Technical Specifications, diagram and description of the Smart Network, technical information sheets for the active equipment of the Smart Network
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements.



RE1.2 Networks dedicated to the communication services of occupants

• • • ► List of ISIA choices:

- Installation of network equipment containers
- Installation of switches
- Activated and administered networkd for future users

The different property units or private spaces may have different levels of network pre-equipment specific to each occupant. It will be based on the international Ethernet-IP standard.

Level 1 requires existence upon delivery of an electrical infrastructure and spaces or containers dedicated to the installation of the electronic network equipment of occupants for their private communication services. Level 2 requires the existence upon delivery of Ethernet network equipment made available to occupants for the local networks of their private communication services. Level 3 requires the existence upon delivery of activated and administered Ethernet networks made available to the occupants for the connection of their communicating systems.

Note: A level of this requirement includes bonus points. They constitute points which are added to the final score and are intended to evaluate projects that include – or have included – the network of users in the construction contract. These bonus points are optional: the non-achievement of the requirements concerned does not prevent obtaining 100% points in the ready2Services label.

• • • ► Level 1 (bonus points): Installation of network equipment containers

This level 1 of the requirement requires the containers in the general distribution room intended to receive the central equipment for the networks and communicating systems of the occupants to be installed during delivery of the building and at least equipped with connection points to a regulated electricity network.

MODES OF EVIDENCE

Level 1

- **Design:** Documents required demonstrating the integration of requirements in the design file.
- **Execution:** As-built technical file and technical information sheets demonstrating the completion of the structures described in the requirements. Examples: Diagrams and descriptions of the Smart Network, technical information sheets.
- **Operation:** Inspection report no more than five years old justifying that the structures described in the requirements are still there. Bonus points are obtained if level 1 has been validated during



• Level 2 (bonus points): Installation of switches

This level of requirement requires that the network in the private spaces be pre-equipped.

It requires:

- Compliance with the previous level of the requirement;
- + the supply and installation of core Ethernet switches of level 3 minimum and access Ethernet switches for the connection of the IP terminals of the future user, of level 2 minimum, according to the brand and model chosen by the future user.

• Level 3 (bonus points): Future users' networks activated and administered

Caution: this level of requirement does not concern the Operation stage.

This level of requirement promotes the "Network as a Service" approach for the rapid installation of the future users in the building.

This level of the requirement covers:

- Compliance with the previous levels of the requirement;
- + the delivery of the activated and administered networks of the future users, ready for the integration of their communicating systems. These networks will be constituted for each future user, according to the choice of the project owner, its architect and the entity appointed to administer the networks, the core Ethernet switches of level 3 minimum and the access Ethernet switches for the connection of the IP terminals of the future user, of level 2 minimum.

In the case where the occupant is also the owner of the building, the occupant's network may be physically common with the Smart Network; in this case it must be logically separated from it.

MODES OF EVIDENCE

Level 2

- **Design and Execution:** same as level 1
- **Operation:** Inspection report no more than five years old justifying the operable condition of the structures mentioned in the requirements. Bonus points are obtained if levels 1 and 2 were validated during completion.

MODES OF EVIDENCE

Level 3

- **Design and Execution:** same as level 1
- **Operation:** not concerned.



RE1.3 Power supply to the communication terminals via the network

- • • ► List of ISIA choices:
 - Protective measures for PoE
 - PoE ports on the access switches
 - Extension capacity of switches
 - Activation of delivery of controllable PoE

Here, the challenge concerns active access equipment connecting IT/communication terminals, which must deliver electrical power over their downlink ports for the equipment attached to them, in accordance with international IEEE (Power over Ethernet) standards.

🔧 Level 1: Protective measures for PoE

Caution: level 1 is not concerned by the Building in Operation stage.

This requirement level evaluates the building's preparation to deliver PoE via network access equipment.

It requires protective measures to be taken to facilitate the future implementation of PoE on the Smart Network (examples: switches with PoE capacity but without providing a PoE power supply, spaces available alongside the switches for adding PoE injectors, the section of the cables of the Smart Network taking PoE into account).

MODES OF EVIDENCE

Level 1

- **Design:** Extract from the specifications describing the protective measures.
- **Execution:** Construction documents demonstrating the application of the protective measures.

🔧 Level 2: PoE ports on the access switches

This requirement level implies that the network access equipment supports the PoE function

It requires:

- The aforementioned Level 1 to be reached
- + the use of switches for access to the Smart Network that have PoE ports.

MODES OF EVIDENCE

Level 2

- **Design:** Extract from the specifications describing the PoE functions for the access switches.
- **Execution and Operation:** Technical information sheets for the access switches justifying their PoE function.



Level 3: Extension capacity of switches

This requirement level concerns network access equipment, which must have an extension capacity of 30% of the number of PoE ports and the overall PoE power that they deliver, as well as the ports and powers used at the time of the delivery of the building.

This level of requirement covers:

- The achievement of the previous levels;
- + the switches of the Smart Network have an extension reserve of 30% applied for each switch in number of PoE ports and in the overall PoE budget.

MODES OF EVIDENCE

Level 3

- **Design:** Extract from the specifications specifying the planned reserve.
- **Execution:** Document specifying, for each switch:
The total PoE power, with the percentage power available in reserve; AND the number of PoE ports in total with the percentage reserve.
- **Operation:** The same document as in Execution, updated no later than 5 years ago.

Level 4: Activation of delivery of controllable PoE

This requirement level implies that the PoE ports of network access equipment are served by a timetable or a third-party system.

It requires:

- The achievement of the previous levels;
- + the activation of PoE delivery, controllable per port using the SNMP protocol.

MODES OF EVIDENCE

Level 4

- **Design:** Extract from the specifications giving the modes of control and delivery of PoE
- **Execution:** Test specifications for the activation / deactivation of the PoE ports of network equipment.
- **Operation:** The same document as in Execution, updated no later than 5 years ago.





RE1.4 Support of the IPv6 protocol

- • • ► List of ISIA choices:
 - Achieved / Not achieved

Support for IPv6 addressing by the Smart Network.

This unique-level requirement is intended to specify the availability of an IPv6 network service for a broadened addressing plan and better security of the Smart Network.

This requirement therefore requires that the active equipment of the Smart Network (including routers and firewall if they exist) support IPv6 addressing, even if this is not necessarily used.

MODES OF EVIDENCE

- **Design:** Extract from the specifications that specifies support of IPv6 for the equipment mentioned in the requirement.
- **Execution:** Technical information sheets for the equipment mentioned in the requirement which specifies IPv6 support.
- **Operation:** Technical information sheets for the network core equipment and for a significant number of access switches which specify support for IPv6.





RE2 - Continuity and functional protection of the Smart Network

RE2.1 Resilience capacity of the building's Smart Network

- • • ► List of ISIA choices:
 - Dual connection of network access equipment
 - Resilience of the redundancy mechanism

The Smart Network supports mechanisms for the detection of network cutouts and self-healing (resilience functions of the local IP networks of the Smart Network).

• • • ► Level 1: Dual connection of network access equipment

This requirement level requires that each item of active equipment for accessing the Smart network has at least two connections with other items of active equipment, ensuring redundant connections and network resilience (examples: the protocols STP, RSTP, MSTP).

• • • ► Level 2: Resilience of the redundancy mechanism

This level of requirement covers:

- the achievement of the previous level;
- + the presence of a redundancy mechanism providing more rapid resilience, of a maximum duration of half a second (examples: LACP protocol with a virtualised core, or G.8032 or MRP).

MODES OF EVIDENCE

Level 1:

- **Design:** Extract from the specifications or diagram which describes the resilience mechanism.
- **Execution:** Technical information sheets for the active equipment of the Smart Network, diagram of the network specifying the redundant links, check the resilience tests and their procedures.
- **Operation:** Check on the resilience tests carried out no more than 5 years ago and their procedures.

Level 2:

- **Design and Execution:** the same as for level 1
- **Operation:** Test report dated no more than 5 years which demonstrates the duration of resilience.



RE2.2 Detection of malfunctions and protection of the Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

Within the connected and communicating building, the network equipment put in place by the owner supporting mechanisms for the detection of malfunctions and able to act automatically on the network ports.

Support for anomaly detection functions on the Smart Network implies the following functions:

- Support for functions for detecting broadcast storms and the emergence of loops, and protection of the network against these types of malfunctions on IP networks.
- Detection and automatic closure of the ports concerned by the malfunction.

This unique-level requirement requires the switches of the Smart Network to have a mechanism which protects the whole of the network in case of malfunction (examples: saturation of a port, port without loop detection device). The mechanism enables at least the reporting of SNMP information to the administrator and closure of the Ethernet port concerned.

MODES OF EVIDENCE

- **Design:** Extract from the specifications which describes the functioning and mechanism for protecting the integrity of the Smart Network
- **Execution:** Technical information sheets for the active equipment of the Smart Network AND functional analysis
- **Operation:** Test report on the protection mechanism OR test procedure OR history of malfunctions with how they were handled.





RE3 - Management of the Smart Network

RE 3.1 Administration of networks and their equipment

• • • ► List of ISIA choices:

- Centralised administration platform for active equipment of the Smart Network
- Support to version 3 of the SNMP protocol
- Administration platform for all equipment of the Smart Network

The network equipment put in place by the owner supporting network administration functions.

• Level 1: Centralised administration platform for active equipment of the Smart Network

This level of the requirement implies that the core and access equipment of the Smart Network be administered on a centralised platform.

It requires all active equipment (network core and access switches) of the Smart Network to report their states and faults to a centralised platform using the SNMP protocol.

This software administration platform enables the centralisation of administration and reports of information and anomalies from *all network equipment*. It may be located on the Smart Network or hosted in the cloud.

• Level 2: Support to version 3 of the SNMP protocol

This level of the requirement requires the administration's authentication and data exchanges to be encrypted.

It requires:

- The achievement of the previous level;
- + the presence of equipment, on the Smart Network, supporting version 3 of the SNMP protocol.

MODES OF EVIDENCE

Level 1 and 2

- **Design:** Extract from the specifications justifying the integration of the requirement
- **Execution:** Technical information sheet for the active equipment AND the platform justifying the integration of the requirement
- **Operation:** Diagram of the Smart Network AND document justifying the correct functioning of the platform (example: screenshots, usage manual, test reports)



- Level 3: Administration platform for all equipment of the Smart Network

This third level of the requirement implies that a centralised platform supervises and administers all elements composing the Smart Network.

It requires:

- the achievement of the two previous levels;
- + the presence of an administration platform specified for the management of *all active equipment* of the Smart Network, including router, firewall, Wi-Fi controller, servers, etc.

MODES OF EVIDENCE

Level 3

- **Design:** Same as level 1
- **Execution:** Usage manual for the administration platform with the functional analysis;
- **Operation:** Same documents as for level 1

RE 3.2 Prioritisation and continuity of network services

- • • ► List of ISIA choices:

- Quality of Service (QoS) function available and activated
- Contractual commitment for a Guaranteed Resolution Time of 8 hours
- Contractual commitment for a Guaranteed Resolution Time of 4 hours
- Contractual commitment to service continuity

The building's Smart Network will have functions and services for prioritising traffic, guaranteeing the bit-rate and the time for intervention and re-establishment of Internet or cloud connectivity in case of a fault.

- Level 1: Quality of Service (QoS) function available and activated

The Quality of Service (QoS) function is available and activated on all active equipment of the Smart Network.

The QoS function can prioritise the processing of the traffic of certain networks in case of network overload.

MODES OF EVIDENCE

Level 1

- **Design:** The supply of required documents justifying the integration of the requirement. Example: Contractual commitment of the operator
- **Execution:** Technical information AND functional analysis sheets justifying the implementation of QoS on the Smart Network.
- **Operation:** Document detailing the QoS rules put in place.



Level 2: Contractual commitment for a Guaranteed Resolution Time of 8 hours

A traffic prioritisation service is put in place on the Smart Network and the connection to the external network limits the period of unavailability of the service to no more than 8h.

This level of requirement covers:

- achievement of level 1;
- + contractual commitment from the operator for a guaranteed bit-rate and a Guaranteed Response Time and Guaranteed Resolution Time of a total of 8h in case of a breakdown in the link of the Internet access provider attaching the network to the general services of the building.

Level 3: Contractual commitment for a Guaranteed Resolution Time of 4 hours

A traffic prioritisation service is put in place on the Smart Network and the connection to the external network limits the period of unavailability of the service to no more than 4h.

This level of requirement covers:

- achievement of level 1;
- + contractual commitment from the operator for a guaranteed bit-rate and a Guaranteed Response Time and Guaranteed Resolution Time of a total of 4h in case of a breakdown in the link of the Internet access provider attaching the network to the general services of the building.

Level 4: Contractual commitment to service continuity

The connected building has a traffic prioritisation service on the Smart Network and a connection to the external network with a theoretical availability rate of 99.999%.

This level of requirement covers:

- achievement of level 1;
- + contractual commitment of the operator for availability of 99.999%.

MODES OF EVIDENCE

Levels 2, 3 and 4

- **Design:** Commitment of the management to fulfil the requirement no later than for the check upon completion.
- **Execution:** Contractual documents specifying the satisfaction of the requirement.

OR, in case of a building delivered without an occupant: commitment by the management to fulfil the requirement at the latest when the building is occupied.

- **Operation:** Contractual documents specifying the satisfaction of the requirement for the connection giving access to the Internet to the Smart Network.



RE 3.3 Common services of the Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The network equipment put in place by the owner supporting the resolution of domain names and the dynamic IP addressing mechanisms for the equipment connected to it.

The aim of this requirement is to set up a function that avoids faults caused by duplicate addresses that may appear during the implementation of static addressing.

MODES OF EVIDENCE

- **Design:** Extract from the specifications specifying the integration of the required functions in the requirement AND specification whether or not there is an obligation to use these functions for each item of equipment connected to the Smart Network.
- **Execution:** Test sheet for the functions mentioned in the requirement OR technical information sheets for these functions.
- **Operation:** Test sheet dated no more than 5 years for the functions



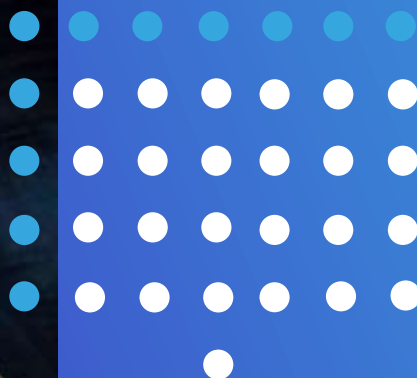


équipement and interfaces

IN1 - Communication interfaces

IN2 - Openness of systems

IN3 - Access to data and services





Equipment and interfaces

This theme consists of relating the equipment, the network and the services through their interoperability, to facilitate the design and operation of the building.

A labelled building is characterised by the interoperability of its systems, meaning by their openness and capacity to function together. The equipment can thus be related inside and outside the buildings, whatever the uses. This interoperability is based on interfaces for access to the services, functions and data of the systems. These are managed by standard Application Programming Interfaces which enable data to be reused by third-party services or applications.

Thanks to interoperability, a labelled building can open the data from the building and make it accessible to optimise the uses of the building. The stability of the services and functioning of communication equipment of the building in degraded mode are also evaluated.

Finally, the implementation of a Building Information Model (BIM) is valorised. This is the digital model for integrating information from the communicating equipment of the building in the form of a database updated at different states of progress of the project, to optimise the management of the building, from its design to operation.

Scale of points per requirement

Title of the requirement	Level	Points
IN1 - Communication interfaces		
IN1.1 Integration of the equipment of the building's Smart Network	Prerequisites: Achieved / Not achieved	/
IN1.2 Capacity of equipment to interface with the Smart Network through their API's	Prerequisites: Capacity of the equipment to interface with an API of the Smart Network	/
	Level 1: Accessibility of API as web services	1
	Level 2: Integration of comfort-management data	5
	Level 3: All connected equipment has an API	7
IN2 - Openness of systems		
IN2.1 Documentation and usage licences for the APIs	Achieved / Not achieved	5

Title of the requirement	Level	Points
IN2.2 Intégration in the digital model (BIM)	Level 1: Integration of data by digital model (BIM)	4
	Level 2: Link between the digital model (BIM) and the exposed equipment	6
IN3 - Access to data and services		
IN3.1 Procedures for access to data and to commands	Achieved / Not achieved	4
IN3.2 Survival of the functions of communicating equipment	Achieved / Not achieved	4
IN3.3 Stability of services	Achieved / Not achieved	4



IN1 - Communication interfaces

IN1.1 Integration of the equipment of the building's Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The communicating equipment of the building must be connected to the Smart Network natively as soon as possible, or via an IP gateway in accordance with international standards. The Smart Network is the building's Ethernet-IP network, as defined in the glossary.

All communicating systems or objects integrated with the building, whatever they are used for, must interface with the Smart Network in accordance with international standards IEEE 802.xx (Ethernet and WiFi) and IETF (IP).

The equipment for the communicating systems and/or objects must integrate into the Smart Network either:

- natively via an Ethernet-IP RJ45 or Wi-Fi interface integrated in the equipment
- via their central equipment
- via a protocol connection gateway in the specific case of peripherals (sensors, actuators, measurement equipment, detectors, etc.,) connected via land line buses (BACnet, LonWorks, Modbus, KNX, ...) or radio (LoRa, Bluetooth, ZigBee, EnOcean...). These land line buses must comply with the corresponding standards.

These prerequisites require all technical equipment of the property asset, and conveyors of services, to be integrated into the Smart Network, either natively or through the intermediary of a gateway.

The aim here is to evaluate the interoperability of the communicating systems and objects with the Smart Network.

Note: It is important to reiterate that the R2S scheme is based on the existence of a unique Ethernet IP for the building, the Smart Network. Therefore, this requirement covers the compliance of the network interfaces of the communicating systems and objects, with the standards defining the TCP/IP, Ethernet and Wi-Fi protocols.

MODES OF EVIDENCE

- **Design:** Extract from the specifications or diagram justifying the existence of the Smart Network and its unifying character.
- **Execution and Operation:** Functional analysis or diagram justifying the existence of the Smart Network and its unifying character.



IN1.2 Capacity of equipment to interface with the Smart Network through their APIs

• • • ► List of ISIA choices:

- Capacity of the equipment to interface with an API of the Smart Network
- Accessibility of API as web services
- Integration of comfort-management data
- All connected equipment has an API

The building's connected equipment must expose its interface data to make it accessible to the services layer. This data may be exposed locally via the building's Smart Network and/or be available in a secure manner over the Internet. In all cases, the equipment producing or using data must describe its interfaces through Application Programming Interfaces (API).

All of the communicating hardware ecosystems of the building must expose their interfacing data to make it accessible to the services layer, transiting via the building's Smart Network (Services Oriented Architecture or SOA).

The data may be exposed either locally on the Local Area Network (LAN) of the building and on the Internet (World Wide Web) using APIs adapted to the services required. The hardware ecosystems that expose their interfacing data (Input / Output) will have APIs.

The APIs must be of the web service type, meaning that they must enable applications to remotely dialogue via the Smart Network and the World Wide Web independently of platforms and the languages on which they are based.

✦ Prerequisites: Capacity of the equipment to interface with an API of the Smart Network

This requirement level evaluates the ability of equipment to interface with an API of the Smart Network; these APIs must be documented and readable

A service-oriented architecture is therefore required for communication. The communicating ecosystems of the building must have APIs for which the documentation is readable in a digital format using a digital tool (such as Swagger).

This prerequisite is applied at least for all of the following categories when the project specifies them:

- telemetry of utilities (examples: potable water, air conditioning, electricity,...),
- regulation of heating and air conditioning.

MODES OF EVIDENCE

All levels

- **Design:** Extract from the specifications that describe the APIs for the categories mentioned in the requirement.
- **Execution and Operation:** API documented in the digital format (accessible with software of the Swagger type).

🔹 Level 1: Accessibility of API as web services

This level of requirement concerns the accessibility of APIs as web services. It requires:

- compliance with the prerequisites;
- + for each of the two categories, the availability of at least one Web service API on the Smart Network at the SOAP, oBIX or JSON RESTful standard.

🔹 Level 2: Integration of comfort-management data

This requirement level extends the same principle to the management of comfort.

It requires:

- compliance with the previous levels
- + the integration of data from the management of comfort or uses per space. For example: lighting, terminal regulation of the air-conditioning, solar blinds,... these examples are not comprehensive.

🔹 Level 3: All connected equipment has an API

This requirement level extends the same principle to all connected equipment of the Smart Network.

It therefore requires:

- compliance with the 3 previous levels
- + the accessibility of all equipment connected to the Smart Network (at least for the available information and possible actions by users in the building) via Web service APIs to the SOAP, oBIX or JSON RESTful standards.



IN2 - Openness of systems

IN2.1 Documentation and usage licences for the APIs

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The Application Program Interfaces (API) must be fully documented in a digital format (usable with software such as Swagger), the conditions for access to this document must be clearly defined and the usage licences described and known.

The usage licences for the APIs must be documented completely and accessible to the owner.

The description of the data will include all parameters and meta data necessary to their use in the programs using these APIs and the usage limits (number of requests per day, reuse of data, etc.)

The usage licences for the APIs (examples: data processing policy, economic models) must be specified and transparent for the owner.

This unique-level requirement requires the usage licences for the APIs to be documented and accessible to owners before contracting.

It concerns evaluating the provision of APIs and a usage license, documented in a digital format and accessible to the owner.

MODES OF EVIDENCE

- **Design:** Extract from the specifications describing the type of licences authorised and the conditions authorised for access to the documentation pursuant to the work contract.
- **Execution:** List of equipment with APIs and licence for each API and the documentation, for which the supply is specified in the work contract.
- **Operation:** Up-to-date list of equipment with APIs and licence for each API and the documentation.



IN2.2 Integration in the digital model (BIM)

• • • ► List of ISIA choices:

- Integration of data by digital model (BIM)
- Link between the digital model (BIM) and the exposed equipment

When a digital model of the building (BIM) exists, the technical systems composing the building's Smart Network and communicating equipment that is attached to it must be described in it.

The digital model (BIM) includes the families of technical systems from the design stage in an interoperable BIM format (example: IFC).

The digital model (BIM) includes at least the information on the division of the building into spaces and rooms and the location of communicating equipment and ecosystems in these spaces.

In order to enable the dynamic monitoring of the systems in the operation stage, a link must be established between the digital model (BIM) and the ecosystems via the intermediary of an API.

• • • ► Level 1: Integration of data by digital model (BIM)

This level of the requirement concerns the integration of communicating systems into the digital model (BIM) from the design.

It therefore requires the digital model (BIM) To integrate the information on the division of the building and the families of equipment for which the sensors and actuators are exposed via an API on the Smart Network.

Level 2 (following page)

MODES OF EVIDENCE

Level 1

- **Design:** Extract of the specifications listing the APIs and plans which represent the equipment concerned AND the BIM agreement describing the divisions.
If the equipment is not present on the plans, the specifications must specify that this task must be done during Execution.
- **Execution:** List of APIs and plans which represent the equipment concerned and the divisions of the digital model (BIM).
- **Operation:** List of APIs and plans which represent the equipment concerned and the divisions of the digital model (BIM). These documents must be dated no more than 3 years unless there has been no development of the installation (revised in case of an update).

❖ Level 2: Link between the digital model (BIM) and the exposed equipment

The aim of this requirement is the existence of a link between the data of the digital model and the information communicated by the equipment exposed on the Smart Network.

The requirement is therefore, at this level:

- compliance with the aforementioned level 1;
- + the existence of a link between the digital model (BIM) and the state of the sensors and actuators exposed via an API on the network.

MODES OF EVIDENCE

Level 2

- **Design:** Extract from the specifications and BIM agreement demonstrating a coordinated structuring of the digital model (BIM) and the meta data available on the sensors and actuators.
- **Execution:** Document comparing the properties of the families in the digital model (BIM) with the documentation for the corresponding API.
- **Operation:** Document dated no more than 3 years comparing the properties of the families of the digital model (BIM) with the corresponding API document (revised in case of an update).



IN3 - Access to data and services

IN3.1 Procedures for access to data and to commands

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The conditions for access to data and commands are described in the APIs. The descriptions must include possible call frequencies, volumes of data supported, the required latency and the availability of subscription mechanisms.

The APIs enabling access to data and commands must have precise specifications.

These give the possible call frequencies per minute / hour / day / month, the volumes of data supported, the number of triggers, the required latency, etc., and the availability of subscription mechanisms.

This unique-level requirement requires the qualification of procedures for data access: The technical conditions for access to the data exposed are clearly identified and documented.

MODES OF EVIDENCE

- **Design:** Extract of the specifications giving the types of licence authorised.
- **Execution:** Document listing the APIs put in place and their licences.
- **Operation:** Document listing the APIs put in place and their licences. The document is dated no more than 3 years and must be up to date with any changes that have been made.



IN3.2 Survival of the functions of communicating equipment

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The hardware ecosystems that are controllable remotely must include a degraded mode of functioning of the building equivalent to manual control in case the building's local network or Internet access is not working.

The objective is to make sure of functional continuity, in a restricted or degraded systems mode, in case of a breakdown of the local network or its Internet connection, for example.

The requirement is that the equipment described by APIs and related to the local functioning of the building must, during a disconnection from the Smart Network and/or cloud services, be able to function autonomously and automatically under the conditions compatible with the continuation of basic functioning of the installations for the users.

IN3.3 Stability of services

- • • ► List of ISIA choices:
 - Achieved / Not achieved

Developments to the services and the APIs that underlie them are controlled by operating contracts between the publishers, equipment manufacturers and other suppliers of services and the owner.

This unique-level requirement requires a guarantee of continuity of operation and stability of APIs.

The servicing and maintenance contracts of the APIs specify their conditions for updates and backwards compatibility.

MODES OF EVIDENCE

- **Design:** Extract from the specifications specifying, for degraded mode:
The equipment considered,
The expected functioning or non-compliance tolerated from nominal functioning.
- **Execution:** Functional analysis specifying the behaviour of the equipment in degraded mode. The document specifies the breakdowns that can be envisaged, the planned functioning in degraded mode and the scenario for a return to normal.
- **Operation:** Test report or test procedure on functioning in degraded mode.

MODES OF EVIDENCE

- **Design:** Commitment of the management to establish a contract as described in the requirement, no later than when the building is in operation.
- **Execution:** Commitment of the management to establish a contract as described in the requirement, no later than when the building is in operation.
- **Operation:** Maintenance contract specifying the elements mentioned in the requirement.





Digital security

**SE1 - Security of networks and
building systems**

**SE2 - Network security
procedures**

**SE3 - Security of access to
services**

SE4 - Protection of data





Digital security

This theme aims to secure the Smart Network and the systems of the building and set up a system for protecting personal data.

By putting data at the heart of the challenge, the connected and communicating building must ensure digital security that is efficient from a technical and organisational point of view. The Ready2Services label provides solutions, taking these two constituents into account:

► The security of access to systems:

The objective is to protect the Smart Network, the active equipment of the network and the services, via authentication mechanisms, monitoring of installations and encryption of communications.

► The security procedures:

Establishing a structured organisation is essential to the functioning of technical requirements. This involves the preparation of procedures for network security, handling of incidents, and prevention and management of risks. The protection of personal data is also evaluated: compliance with the General Data Protection Regulation (GDPR) is required, applicable since 25 May 2018 in France and in Europe, which is aimed at creating a framework of digital trust on the protection of data.

Scale of points per requirement

Title of the requirement	Level	Points
SE1 - Security of networks and building systems		
SE1.1 Authentication mechanisms to access to the Smart Network	Prerequisites: Functions supported by the access switches	/
	Level 1: Connections to the Smart Network with request for authentication	2
	Level 2: Presence of a centralised network platform	3
SE1.2 Conditional routing of the Smart Network mechanisms	Achieved / Not achieved	3



Title of the requirement	Level	Points
SE1.3 Support for VLAN	Level 1: Isolation of IT/communication terminals"	1
	Level 2: Isolation of IT/communication terminals based on their function and location"	2
	Level 3: Configuration of the assignment of VLAN"	3
	Level 4: Configuration of the connection of non-registered equipment	4
SE1.4 Mechanisms for traffic monitoring and protection against malware	Achieved / Not achieved	3
SE1.5 Encryption of communications	Achieved / Not achieved	4
SE2 - Network security procedures		
SE2.1 Monitoring flows and configurations of the Smart Network	Achieved / Not achieved	3
SE2.2 Processing incidents and alert chain	Achieved / Not achieved	2
SE2.3 Equipment software update	Achieved / Not achieved	2
SE3 - Security of access to services		
SE3.1 Securing access to applications	Achieved / Not achieved	3
SE3.2 Prevention and management of risk	Achieved / Not achieved	2
SE4 - Data protection		
SE4.1 Compliance with the General Data Protection Regulation	Prerequisites: Achieved / Not achieved	/



SE1 - Security of networks and building systems

SE1.1 Authentication mechanisms to access to the Smart network

• • • ► List of ISIA choices:

- Functions supported by the access switches
- Connections to the Smart Network with request for authentication
- Presence of a centralised network platform

The downlink ports of the network equipment will support mechanisms for the authentication of systems that are, or would like to be, connected to it, in accordance with international standards for network security in force.

At level 1, all of the equipment and users wishing to connect to the Smart Network must first be authenticated before any opening of the network session.

The use of certificates is mandatory for remote access to the Smart Network. As a minimum, passwords must mandatorily be hashed.

All unused ports of switches or ports on which no network session is active must be logically closed (except in the case of reasoned exceptions).

At level 2, it adds an AAA (Authentication, Authorization and Accounting) platform of the RADIUS (Remote Authentication Dial-In User Service) type for centralising the management of access to the Smart Network, whether this is done locally or remotely.

The identifiers of the users of the AAA platform may be correlated with those of the access-control platform at the application level of systems, in order to avoid repeated authentication (Single Sign-On (SSO)). The use of two-factor authentication is mandatory for remote access to the Smart Network.

Note: Authentication is a stage that consists of checking the legitimacy of a user and/or communicating equipment before any integration into the Smart Network or a VLAN and before the assignment of an IP address.

• • • Prerequisites: Functions supported by the access switches

Support, via the switches, for access to functions:

- Support for ACL (Access Control List)
- IEEE 802.1X in mode MAC-based and User-based, related to an ACL or an AAA (Authentication, Authorization and Accounting) platform

MODES OF EVIDENCE

Prerequisites:

- **Design:** Extract from the specifications describing the characteristics of the active equipment of the network. Or technical information sheet for the envisaged equipment.
- **Execution:** Technical information sheets for the active equipment of the network, certifying the capacity of the hardware.
- **Operation:** Technical information sheets for the active equipment of the network, certifying



Level 1: Connections to the Smart Network with request for authentication

This level requires:

- compliance with the prerequisites;
- + the presence of a secure means of providing named connections to the Smart Network from other networks (example: Internet). This secure equipment authenticates remote and local IT/communication users and terminals and encrypts data.

MODES OF EVIDENCE

Level 1:

- **Design:** Extract from the specifications describing the implementation of the required functions.
- **Execution:** As-built technical file, test results and technical information sheets demonstrating the completion of the structures described in the requirements.
- **Operation:** Functional analysis describing the implementation of the required functions. OR test report on these functions.

Level 2: Presence of a centralised network platform

This requirement level enables easy management of secure access to the Smart Network, made possible by the use of a centralised authentication platform.

It therefore requires:

- compliance with the previous levels;
- + the presence of a centralised network platform for authentication, authorisation and accounting (AAA, example: RADIUS (Remote Authentication Dial-In User Service) enabling the implementation of the functions detailed in the description of the requirement (management of identifiers, verification mechanism,...).

MODES OF EVIDENCE

Level 2:

- **Design:** Extract from the specifications describing the centralised authentication platform and the functions detailed in the description.
- **Execution:** Technical information sheet for the centralised authentication platform justifying the integration of the functions detailed in the description.
- **Operation:** Same as level 1



SE1.2 Conditional routing mechanisms of the Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The Smart Network supports conditional routing mechanisms (example: inter-VLAN routing).

This unique-level requirement requires the routing process to be managed by the core of the Smart Network. It will be done conditionally, according to one or more of the following conditions:

- the direction of initiation of the data exchange,
- the network of origin and/or destination (VLAN, LAN, WAN),
- the IP address of the sender and/or addressee,
- the protocol used,
- any other appropriate condition.

MODES OF EVIDENCE

- **Design:** Extract from the specifications showing the inclusion of requirements in the design file.
Examples: Special Technical Specifications.
- **Execution:** Documents establishing the results of tests and technical information sheets demonstrating the completion of the structures described in the requirements.
Examples: Conditional routing test documents, technical information sheets for equipment.
- **Operation:** Supply of an up-to-date conditional routing table, test report on





SE1.3 Support for VLAN

• • • ► List of ISIA choices:

- Isolation of IT/communication terminals
- Isolation for IT/communication terminals based on their function and location
- Configuration of the assignment of VLAN
- Configuration of the connection of non-registered equipment

Each communicating system and user profile connected to the Smart Network must be isolated in one or more virtual networks.

Each hardware ecosystem and object connected with the same usage will have its own virtual networks (VLAN, Virtual Local Area Network). All of the access equipment and the core of the Smart Network supports the standard IEEE 802.1q.

The VLAN must be able to be assigned either:

- Statically by a prior configuration of the attached report and after checking the MAC or IP address presented by the terminal against a list of authorised addresses;
- Dynamically after authentication of the connected terminal and/or user.

The VLAN must be able to be assigned according to the following levels:

- On the network layer, the physical port of connection of the network equipment;
- On the network layer according to the MAC (Medium Access Control) address presented by the host;
- On the network layer according to the IP address presented by the host.

• • • Level 1: Isolation of IT/communication terminals

The Smart Network is partitioned to isolate the IT/communication terminals according to defined criteria.

• • • Level 2: Isolation of IT/communication terminals based on their function and location

- Compliance with the aforementioned level 1;
- + the partitioning must isolate the IT/communication terminals based on their functions and their location (grouping by function and space). The servers attached to the Smart Network are also isolated from the terminals.

MODES OF EVIDENCE

All levels

- **Design:** Extract from the specifications describing the planned equipment or function. Examples: Special Technical Specifications, technical information sheets
- **Execution:** Functional analysis describing the implementation of the required functions. Examples: Technical information sheets,



• Level 3: Configuration of the assignment of VLAN

- Compliance with the previous levels;
- + the assignment of VLAN must be configured automatically according to the IT/communication equipment or user connected (IEEE 802.1ak) with the secure mechanism (example: 802.1X) and not based on a MAC or IP address.

• Level 4: Configuration of the connection of non-registered equipment

- Compliance with the previous levels;
- + the connection to the Smart Network of a non-registered item of equipment is either accepted while giving it access to limited resources which must be determined, or rejected.

- **Operation:** Functional analysis describing the implementation of the required functions.
OR test report on these functions.



SE1.4 Mechanisms for traffic monitoring and protection against malware

• • • ► List of choices:

- Achieved / Not achieved

The core network equipment and the main distribution nodes of the connected building support mechanisms for monitoring traffic and protecting against malware. For this, they have a firewall and anti-malware software, which provides better protection for the Smart Network and the communicating equipment exposed.

This unique-level requirement requires incoming and outgoing traffic on the Smart Network to be monitored by a firewall with:

- a system for examining frames and for identifying and blocking suspect content,
- as well as anti-malware software concerning the opening of the building's Smart Network to the exterior.

Any local interconnections between the Smart Network and the networks of occupants must be implemented through the firewall of the Smart Network.

Only authorised communication ports must be opened on the routers of the Smart Network; all the others must be closed.

MODES OF EVIDENCE

All levels

- **Design:** Documents required demonstrating the integration of requirements in the design file
- **Execution:** Documents required, results of tests and technical information sheets demonstrating the completion of the structures described in the requirements. Examples: Technical information sheets for the firewalls, test procedures
- **Operation:** Document justifying the presence of a firewall on the Smart Network AND a procedure for updating equipment. Examples: Test procedures.



SE1.5 Encryption of communications

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The core equipment of the network and the main distribution nodes support a mechanism for encrypting data exchanges, which can protect against the interception of communications.

The requirement covers, through the connection protocol and the network equipment, the support of a mechanism for encrypting exchanges of data taking place on the intra-building networks and the external networks in general.

If they exist, the land line networks of the Smart Network have a reliable security mechanism: WPA2 CCMP or VPN). AND all exchanges of data between the Smart Network and other networks are secured (example: SSL, TLS, TTLS, https...).

Note: this requirement does not apply to "guest" equipment on the network which does not have direct access to other equipment (example: "guest" on the Wi-Fi network that only accesses the Internet).

MODES OF EVIDENCE

- **Design:** Extract from the specifications describing the security measures provided for the land line networks of the Smart Network if they exist AND those provided for the interconnections with other networks.
- **Execution and Operation:** Functional analysis describing the security measures put in place for the land line networks of the Smart Network if they exist AND those put in place for the interconnections with





SE2 - Network security procedures

SE2.1 Monitoring flows and configurations of the Smart Network

- • • ► List of choices:
 - Achieved / Not achieved

A map of the Smart Network is made to determine the expected flows. A traffic analysis can then check that the traffic on the Smart Network does correspond to that expected, and thus prevent malfunctions or intrusions. The network configurations are also checked.

This unique-level requirement requires a map of the Smart Network to be produced, as well as the presence of tools for monitoring configurations, architectures and flows on the Smart Network.

The Smart Network's administration platform has:

- a graphical interface of the map of the network,
- a tool listing the logical configuration change history of the network,
- a tool for monitoring traffic load on the logical networks.

A procedure exists to take into account flows found on the Smart Network that are not identified in the map.

MODES OF EVIDENCE

- **Design:** Map of the network representing the equipment and flows expected. A diagram which does not represent the flows is not sufficient. AND procedure for handling unexpected flows.
OR extract from the specifications describing the implementation of the map AND the procedure used for implementation.
- **Execution:** Map of the network representing the equipment and flows expected. AND functional analysis demonstrating the implementation of network filtering and/or flow monitoring based on the map.
AND procedure for handling unexpected flows.
- **Operation:** Map of the network representing the equipment and flows expected. The document must be updated no more than a year ago.
AND test report demonstrating the correct functioning of filtering and/or flow monitoring based on the map.
AND procedure for handling unexpected flows.



SE2.2 Processing incidents and alert chain

- • • ► List of ISIA choices:
 - Achieved / Not achieved

Caution: this requirement concerns only the Building in Operation stage.

The owner of the connected and communicating building has an organisation and procedures for handling incidents related to the Smart Network, to the technical systems that are connected to it and to the services that it delivers.

The requirement covers the existence of an organisation and a procedure for handling incidents: Specify procedures for collecting information through logs of alarms and events, alert procedures and the management and resolution of incidents.

MODES OF EVIDENCE

- **Operation:** Procedure for the detection and handling of incidents, test report

SE2.3 Equipment software updates

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The owner of the building and/or the operator that it will have designated has formalised procedures for updating equipment and software in the systems of the Smart Network.

The requirement covers the existence of formalised procedures for updating equipment and software of the systems of the Smart Network. These updates may cover firmware for equipment, software, licenses, drivers, operating systems, security policy, antivirus definitions,...

MODES OF EVIDENCE

- **Design:** Extract from the specifications describing, for the Execution stage, the requirements relative to the application of updates for the company until acceptance test of its projects AND the production of an update guide for the use of the operator.
- **Execution:** Update guide listing all equipment and software with the version applied at the time of delivery of the projects.
- **Operation:** Update guide listing all equipment and software with the version applied and the date of the last search for an update, which must be dated no more than one year.



SE3 - Security of access to services

SE3.1 Securing access to applications

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The digital services and applications accessible to the various users of the building have secure communication. For this, the secure communication mechanism must include the use of firewalls and encryption mechanisms.

This unique-level requirement, which has the status of a prerequisite, requires that the APIs exposed on the Smart Network be accessible and secure from end to end (radio and land line). This provision means that only the people who communicate can read the exchanged messages, without any need to add intermediate security mechanisms between these persons.

Note: The achievement of this requirement does not mean that other means of security specified for other requirements of the scheme do not need to be implemented.

MODES OF EVIDENCE

- **Design:** Extract from the specifications describing the implementation of a means of establishing secure communication from end to end on the Smart Network from one or more external networks.
This document must also take into account equipment that may be directly connected to their manufacturers and for which the flows may not be analysed by the firewall.
- **Execution:** Functional analysis AND technical information sheet on the means of establishing secure end to end communication on the Smart Network from one or more external networks.
This document must also take into account equipment that may be directly connected to their manufacturers and for which the flows may not be analysed by the firewall.
- **Operation:** Document listing the connections on the Smart Network from external networks and the means of securing each one from end to end. The document must have been updated no more than a year ago.
This document must also take into account equipment that may be directly connected to their manufacturers and for which the flows may not be analysed by



SE3.2 Prevention and management of risks

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The owner of the building and/or the operator that it will have designated must have established a procedure for managing and preventing risks, including:

- The management of access permissions for users and programs,
- The procedures for managing risks for access to the services of the building on the Smart Network.

This unique-level requirement covers the existence of an IT charter/procedure for managing and preventing risks. This document at least includes the management of access permissions.

MODES OF EVIDENCE

- **Design:** Extract from the specifications specifying, for the Execution stage, management of access permissions on the described systems.
- **Execution:** Functional analysis specifying the management of access permissions on the systems put in place. This document must be usable when it is used in the Building in Operation stage.
- **Operation:** Description of the organisation and the procedure for managing access permissions on the systems of the Smart Network





SE4 - Data Protection

SE4.1 Compliance with the General Data Protection Regulation

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The owner of the building must have checked the compliance of its smart system with the regulations concerning data protection:

- And, from 25 May 2018, application of regulation 2016/679 from the European Parliament and Council dated 27 April 2016 relative to the protection of natural persons with regard to the processing of private data and the free circulation of this data, abrogating directive 95/46/CE, known as the General Data Protection Regulation or GDPR.

This unique-level requirement, which has the status of prerequisite, requires the existence of a document justifying compliance with the legislation on the protection of personal data.

MODES OF EVIDENCE

- **Design:** Commitment of the project owner to produce the document mentioned in the requirement.
- **Execution:** Document mentioned in the requirement, or commitment from the project owner to produce it.
- **Operation:** Document mentioned in the requirement.







Responsible management

MA1 – Project governance

MA2 – Property ownership

MA3 – Framework for services contracting

MA4 – Environmental qualities

MA5 – Management system





Responsible management

The theme "Responsible management" includes several aspects. It includes establishing governance of the project, commissioning, a framework for contracting, reflection on property ownership and on the environmental challenges of the connected and communicating building, in order to combine the environmental and digital transitions. The theme proposed by the R2S-Ready2Services label is a project management tool which can respond to the governance challenges posed by the arrival of digital technology in the building. These challenges can be summarised in three constituents:

► **Project governance:** includes elements relative to the acceptance testing and administration of the Smart Network and to requirements concerning the proper management of the project.

► **The ownership of data and the contracting of services:** the objective is to foster reflexion around the ownership of data and the infrastructure of the Smart Network. A framework for contracting concerning the conditions for access to services is also present.

► **The environmental qualities:** including requirements related to the environmental footprint of electronic equipment present in the building through the intermediary of PEP sheets, and the measurement of electromagnetic fields.

Scale of points per requirement

Title of the requirement	Level	Points
MA1 – Project governance		
MA1.1 SMART information in the contractual documents	Level 1: Presence of Smart information	2
	Level 2: Presence of a Smart Section	4
MA1.2 Administration of the Smart Network	Achieved / Not achieved	2



Title of the requirement	Level	Points
MA1.3 Acceptance testing of the Smart Network	Level 1: Acceptance testing of the cabling of the Smart Network	2
	Level 2: Configuration of the active equipment of the Smart Network	3
	Level 3: Security test protocols on the Smart Network	4
	Level 4: API test protocol	5
MA2 - Property ownership		
MA2.1 Infrastructure ownership	Achieved / Not achieved	2
MA2.2 Data ownership	Achieved / Not achieved	2
MA3 - Framework for services contracting		
MAN3.1 Services contracts (SLA) with suppliers	Achieved / Not achieved	2
MA4 – Environmental qualities		
MA4.1 Determination of the electromagnetic field and provisions taken	Prerequisites Achieved / Not achieved	/
MA4.2 Supply of PEP environmental sheets	Achieved / Not achieved	3
MA5 - Management system		
MAN5.1 Project management	Prerequisites Achieved / Not achieved	/
MA5.2 Implication of stakeholders	Level 1: Processing complaints	1
	Level 2: Consultation of stakeholders	2
	Level 3: Satisfaction surveys	3



MA1 – Project governance

MA1.1 SMART information in the contractual documents

- • • ► List of ISIA choices:
 - Presence of Smart information
 - Presence of a Smart Section

Caution: this requirement does not apply to the Building in Operation stage.

The information related to the implementation and operation of the communicating building must be presented in the contractual documents.

"Smart" corresponds to all hardware and application solutions, and the implementation, coordination and operation service used to make the building communicating.

This requirement demands the presence of information on "smart" elements, meaning those present in the technical specifications for the equipment, infrastructure and services in accordance with Ready2Services requirements.

It is a cross-functional section, which is intended to coherently handle mixed and multi-technology systems.

The perimeter of the Smart Section must be determined by the project owner.

- Level 1: Presence of Smart information
Presence of "smart" information in the contractual documents for the contract (special technical specifications,...).
- Level 2: Presence of a Smart Section
Presence of a "smart" section or appendix.

MODES OF EVIDENCE

- **Design and Execution:**
Contractual documents demonstrating the integration of elements described in the requirement.
Example: Special Technical Specifications





MA1.2 Administration of the Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The Smart Network, the data and the APIs are administered by a named entity.

A Ready2Services building must have an infrastructure and a Smart Network for the connection of the communicating systems of the building. In order to maintain the level of service and security of the whole over time, an entity must be appointed to administer the Smart Network, the data and the APIs which are exposed on it.

MODES OF EVIDENCE

- **Design:** Extract from the specifications which imposes an administration role in the installation of the Smart Network during the Execution stage
- **Execution:** Documents demonstrating the presence of a Smart network administrator for its installation.
Examples: organisation chart, administrator contract, documents produced by the administrator
- **Operation:** Documents demonstrating the presence of an administrator of the Smart network, data and APIs.
Examples: organisation chart, administrator contract, documents produced by the administrator





MA1.3 Acceptance testing of the Smart Network

- • • ► List of ISIA choices:
 - Acceptance testing of the cabling of the Smart Network
 - Configuration of the active equipment of the Smart Network
 - Security test protocols on the Smart Network
 - API test protocol

The Smart Network and its active equipment must be accepted.

- Level 1: Acceptance testing of the cabling of the Smart Network
- The acceptance of the cabling of the Smart Network is tested.

MODES OF EVIDENCE

Level 1

- **Design:** Extract from the specifications demonstrating the inclusion of new requirements AND the planned test protocols.
- **Execution:** Acceptance testing documents AND results of tests justifying the achievement of the level. These documents must contain only positive results (no failed tests).
- **Operation:** Result of the acceptance test of the network dated no more than 10 years. For connections created since the previous check: same modes of evidence as during Execution.





Level 2: Configuration of the active equipment of the Smart Network

The requirement covers:

- compliance with the aforementioned level 1
- + compliance with the specifications and the functional analysis of the configuration of the active equipment of the Smart Network is checked.

MODES OF EVIDENCE

Level 2

- **Design:** same as level 1.
- **Execution:** same as level 1.
- **Operation:** Document justifying the correct functioning of the Smart Network and the update to the configuration of the active equipment according to requirements



🔹 Level 3: Security test protocols on the Smart Network

- compliance with the previous levels;
- + the level of security is proven with the writing and implementation of a test protocol for the security measures put in place on the Smart Network and the equipment connected to it.

MODES OF EVIDENCE

Level 3

- **Design:** same as level 1.
- **Execution:** same as level 1.
- **Operation:** Result of the latest test dated no more than 3 years ago.

🔹 Level 4: API test protocol

- compliance with the previous levels;
- + the exposure of APIs on the Smart Network is proven with the writing and implementation of a test protocol for the APIs put in place.

MODES OF EVIDENCE

Level 4

- **Design:** same as level 1.
- **Execution:** same as level 1.
- **Operation:** Result of the latest test dated no more than 3 years ago in case of creation or update to APIs.





MA2 - Property ownership

MA2.1 Ownership of the infrastructure of the Smart Network

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The network infrastructure of the building must be included within the perimeter of the property ownership.

This unique-level requirement covers the integration of the infrastructure of the Smart Network within the perimeter of the property ownership.

MODES OF EVIDENCE

- **Design and Execution:** Document establishing the ownership of the Smart network (active equipment of the network and cabling). Example: commitment by the project owner
- **Operation:** Document establishing the ownership of the Smart network (active equipment of the network and cabling).

MA2.2 Ownership of data

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The ownership of data coming from the equipment connected to the Smart Network must be defined. This concerns both generated data and data stored on equipment connected to the Smart network.

The data concerned is that coming from equipment serving the control functions of the building (sensors, actuators, programmable controllers,...) as well as data coming from information reports from hardware ecosystems serving common functions such as the signalling of alarms, breakdowns or malfunctions, video surveillance images, etc.

MODES OF EVIDENCE

- **Design and Execution:** Document specifying the ownership of data. Example: commitment from the project owner
- **Operation:** Document specifying the ownership of data.





MA3 - Framework for services contracting

MA3.1 Service level agreements (SLA) with suppliers

- • • ► List of ISIA choices:
 - Achieved / Not achieved

This requirement covers the existence of Service Level Agreements with suppliers of services defining the nature and conditions for access to services provided by the Smart Network.

All of the network infrastructure, communicating systems and services of the building must be the subject of a service level agreement.

Nature of the guarantee:

- Duration of the guarantee and of the support;
- Service level (perimeter, period for the resolution of problems and resources used);
- Type of commitment (resources or results);
- Services included in the guarantee and additional payable services;
- Conditions for the continuation of operation in case of default (example: escrow agreement for the software).

Note: Service contracts are essential and also concern property services, meaning services added or routed over the building's Smart Network on request from the tenant or future user.

MODES OF EVIDENCE

- **Design:** Extract from the specifications providing for an impact in the Execution stage due to the establishment, during the works, of a service contract at the initiative of the future operator.
- **Execution:** Document justifying the present or future existence of a service contract at the initiative of the operator.
- **Operation:** Document justifying the existence of a service contract.





MA4 – Environmental qualities

MA4.1 Determination of the electromagnetic field and provisions made

- • • ► List of ISIA choices:
 - Achieved / Not achieved

Caution: this requirement only applies to the Building in Operation stage.

This requirement requires the determination of electromagnetic fields in the premises. This evaluation is based on the instructions of the 2013/35/EU Directive of 26th June 2013 relative to the exposure of workers to risks related to physical agents (electromagnetic fields).

The 2013/35/EU Directive aims to define the rules for preventing risks to the health and safety of workers exposed to electromagnetic fields, notably against their direct biophysical effects and their known indirect effects. It thus aims to improve the protection of the health and safety of workers, which until then was based solely on general preventive principles, and includes a graduated approach to means of prevention and internal dialogue to be implemented in case of an overrun of the "action values" and "limit values".

The 2013/35/EU Directive must be transposed in national law of each member state of the EU until 1st July 2016. The project must therefore refer to the local transposition of this Directive to validate the requirement.

This level, of the status of prerequisite, requires at least compliance with the regulation (transposition of the 2013/35/EU Directive) concerning the perimeter related to the requirements of the R2S scheme (equipment, network,...). The requirement is also achieved if the regulations as a whole are applied.

MODES OF EVIDENCE

- Operation: Document certifying the application of the regulations on electromagnetic fields. This document must include elements on the evaluation of risks related to the electromagnetic fields, at least on the scope of R2S, and the measures taken in case the thresholds are exceeded (see the regulations on the limit values for exposure and the values for triggering actions). As specified in the regulations, the evaluation of risks may be done from documentary data (technical information sheets for radiating equipment, for example), measurements, calculations or digital simulations.



MA4.2 Supply of PEP environmental sheets

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The building must provide at least one PEP environmental sheet for an item of equipment of the Smart Network or one that is connected to it.

A Product Environmental Profile (PEP) is an environmental identity card for an item of electrical, electronic or climatic engineering equipment. It defines the environmental profile of a product based on the results of the life-cycle analysis of the product studied, taking into account, for example, the implementation and operation of the product, the transport and raw materials used in making it.

The objective of a PEP is to provide information on the functioning and service life of the product in the structure, with notably:

- The technical characteristics of the product (functional unit, constituent materials,...),
- The environmental impact, taking into account the stages of manufacture, distribution, installation, usage and end of life.

An environmental declaration must be established by the entity responsible for marketing construction and decoration products as well as electrical, electronic and climatic engineering equipment intended for sale to consumers when a communication of an environmental character accompanies the marketing of these products. There are two orders on the environmental performance of equipment, one covering the environmental declaration of equipment intended for the building and the other covering the procedures for verification.

In the context of the scheme, at least one PEP sheet is required on at least one item of "smart" equipment present in the building. The following elements are considered as forming part of the Smart Section: High-current wiring, low-current wiring, HVAC, joinery work, motors, access control and security.

This unique-level requirement covers knowing the environmental impact of the project, through the supply of at least one PEP environmental sheet for equipment exposed natively on the Smart Network or equipment that is connected to it via an IP gateway.

MODES OF EVIDENCE

All levels:

PEP environmental sheet for an item of equipment on the Smart Network or an item of equipment connected to it natively or via an IP gateway.



MA5 – Management system

MA5.1 Project management

- • • ► List of ISIA choices:
 - Achieved / Not achieved

The Project Owner has a central role in the implementation, monitoring and improvement of the management of the project, but its partners (architect, contractors,...) are also involved. It is important that all those involved in the project, primarily the Project Owner stakeholders, be fully informed of the objectives and resources of the project.

It is for each Project Owner to define the organisation, skills, methods, resources and necessary documentation to meet its objectives and requirements of the present scheme.

In order to efficiently manage the labelling project, project management must be set up, which includes:

- A commitment from the management

The commitment from the management of the applicant organisation on the project is established, formalised by a document signed by the management, specifying:

- ✓ The performance objectives targeted for the operation in terms of overall level (based on 3 stars) are chosen and ranked,
- ✓ The setting up of resources and adequate means for the proper completion of the project,
- ✓ As well as the main functional objectives of the project.

The commitment document must be disseminated to all employees and stakeholders in the project. In case of a modification of the performance objectives targeted, it must be revised and redistributed.

- The description of the roles, responsibilities and authorities

The breakdown of missions, responsibilities and authorities must be defined in writing and the employees and stakeholders must be informed of them. This breakdown of missions is in line with the scheduling of the project.

The roles, responsibilities and authorities of each player or stakeholder in the project are defined in relation with the schedule established for each stage or period concerned. It must be communicated to the persons concerned.

- The planning of actions

The applicant describes the succession of steps in each stage of the project, or each period in operation, identifying the following organisational elements: the actions and activities, the timetable, the responsibilities and associated authorities, the interfaces between stakeholders, the resources, methods and documents to be used, the procedures for the evaluation of performance and the documented information to be retained.





Project review meetings are programmed so as to check the key steps in achieving the targeted performance, or to react in time and in a proportionate manner so that it is achieved.

- Evaluation of the performance of the project in relation to objectives targeted

An evaluation of the performance of the project in relation to the objectives targeted is carried out at key steps (program, design, execution) or periodically in the operation stage, from its entry into certification, and documented.

- The implementation of corrective actions in case of non-compliances

When an expected performance is not achieved, or the management system is not working as planned, a corrective action is implemented in order to correct the non-compliance, if possible.

The non-compliances observed, both on the performance of the building and on the functioning of the management system, are the subject of corrective actions, without it being necessary to set up a dedicated procedure.

This unique-level requirement with the status of prerequisite requires a definition of the project management. The management thus takes a quality-based approach, controlling the project overall.

MODES OF EVIDENCE

All stages

Commitment of the management in order to apply the approach in the project:

Commitment document from the applicant, dated and signed by the management

Proof of the transmission of this commitment to the stakeholders in the project

The description of the roles, responsibilities and authorities:

Organisation chart, engagement letter, minutes of meeting, etc., for each stage concerned or for the project, possibly contracts, task distribution list, etc.

Planning the actions for the project:

Planning documents for the project for each stage.

Project review planning document.

Minutes of meetings and reviews.

Evaluation of the performance of the project:

ISIA evaluation tool completed, with substantiating documentation.

The implementation of corrective actions in case of non-compliances:

List of non-compliances, corrective actions and results.





MA5.2 Involvement of stakeholders

- • • ► List of ISIA choices:
 - Processing complaints
 - Consultation of stakeholders
 - Satisfaction surveys

It is requested that stakeholders* be consulted throughout the entire project.

* The stakeholders are the users.

🔹 Level 1: Processing complaints

This level of the requirement covers the processing of complaints: Complaints from stakeholders are recorded and processed, at all stages.

🔹 Level 2: Consultation of stakeholders

This level of the requirement covers:

- compliance with the aforementioned level 1;
- + the consultation of stakeholders: The stakeholders are consulted at key stages of the project and their opinions are taken into account as far as possible. The key stages are to be defined by the project initiator in accordance with the complexity of the project.

🔹 Level 3: Satisfaction surveys

This level of the requirement covers:

- compliance with the previous levels;
- + the implementation of a satisfaction survey: The satisfaction survey is done in such a way as to identify expectations, subjects of satisfaction and dissatisfaction. As digital technology is developing rapidly, satisfaction must also be evaluated in time to understand requirements and orient these developments towards greater client satisfaction.

MODES OF EVIDENCE

All stages

- Level 1: Document for recording and processing complaints
- Level 2: Consultation media, reports
- Level 3: Media for the satisfaction survey, results, reports



 **services**

SE1 Energy services





Services

This theme evaluates the installation of an energy monitoring platform.

Comment: The Ready2Services labelled building enables the installation of a multitude of services (see the non-comprehensive list opposite on the right for examples); however, setting these up must be put into context with regard to the activity of the building and the expectations of its occupants. The Ready2Services label is not intended to impose the installation of specific services, therefore only the energy service is present, given that it is a concern common to all buildings, whatever their situation.

► services to the building:

- energy services;
- maintenance and operation services (preventive or even predictive maintenance, control and management of installations, management of the life-cycle of installations);
- space development services (space planning, transformation of the use of a building, management of furniture);
- management of waste and cleanliness;
- safety, security.

► services to occupants:

- general services, concierge services, inter-company restaurant, room reservation,...);
- well-being and health services.

Scale of points per requirement

Title of the requirement	Level	Points
SE1 - Services énergétiques		
SE1.1 Mise en place d'une plateforme de suivi énergétique	Achieved / Not achieved	6



SE1 - Energy services

SE1.1 Installation of an energy monitoring platform

The building sets up a platform for monitoring energy consumption.

This service must enable centralisation of the building's energy information and be able to define its consumption/production profile.

It must enable the building to be opened to energy flexibility and is one of the tools for dialogue with the energy grid (SmartGrid).

We may refer to the standard NF EN 16-001: Energy Management Systems – requirements and guidelines for the use according to NF EN ISO 50.001 and the method PDCA – Plan|Do|Check|Act] – [2009] and standard NF EN 15-900: Energy Efficiency Services – Definitions and requirements [2010].

This platform must:

- enable real-time monitoring of the evolution of consumption of the building, and archive and keep the history of trend monitoring to facilitate the analysis and definition of the energy or environmental profile (carbon footprint, energy performance) of the site.
- include tools for analysis and with decision-making, to facilitate controlling performance.
- have a user-friendly and ergonomic user interface with different levels of access to enable its use by different types of users (Asset manager, Property manager, Building manager, Occupants).
- enable monitoring by comparison.
- make it possible to create personalised key performance indicator reports for the user.
- display complete connectivity on the R2S by the use of APIs and/or services for direct access to the site's data (such as the technical building management system) and to external data (particularly weather data: météoNorm).

This platform may be hosted locally.

This unique-level requirement demands the implementation of an energy monitoring platform in accordance with the above description.

The objective of this requirement is to better control the energy consumption of the building.

MODES OF EVIDENCE

- **Design:** Specifications describing the functions to be put in place compliant with the description of the requirement.
- **Execution:** Functional analysis AND test reports for the platform.
- **Operation:** Report on the functioning of the platform and annual overview dated no more than one year.



Glossary



API

An API (Application Programming Interface) is a standardised set of classes, methods or functions in a Web Service, by which software offers services to other software, without one knowing the internal functioning of the other.

Service-Oriented Architecture (SOA)

The service-oriented architecture is an approach for creating an architecture based on the use of services. These services (such as RESTful web services) fulfil small functions, such as the production of data, the validation of a client or the provision of simple analyses.

SOA in fact consists of reviewing existing architectures and treating most of the main systems as services, extracting them to gather them in a single domain where they are prepared as solutions.

One of the keys to SOA architecture is that the interactions take place with modular services (flexible coupling), which function independently. SOA enables the services to be reused, which avoids starting from zero when upgrades and other changes are necessary. It is an undeniable advantage for buildings that seek to save time and money.

BaaS

BaaS stands for "Building as a Service", which means a building transformed into a service platform.

BIM

BIM (Building Information Modelling) is a unified description format of a building or building structure, stored in a database structured locally or in the cloud, containing all technical information necessary to its design, construction, maintenance, repair, modification or demolition. In its active version, the data from communicating ecosystems is related dynamically to the BIM, so that the BIM is literally the digital twin of the physical building, being updated in real-time.

Standardised cabling

Cabling including twisted-pair links able to support typical connections (xDSL, Ethernet First Mile, analogue and digital links) and optical fibres able to support broadband Ethernet protocols standardised by the IEEE or the PON family standardised by the ITU, between the general distributor and the utility rooms or the connection nodes for each zone or floor.





Smart Network Cabling

This is the unique cabling gathering all physical links for the communication systems of the general services integrated into the building.

Network map

A map of an IT network is a representation of this network that may include different elements such as network active equipment, equipment connected to it, software installed and their versions, processes, flows between these devices and links with third-party networks such as the Internet. This representation can distinguish infrastructure from the application part.

The map can inventory the components of the network, with the aim of having better control of them. This control can improve the digital security of the network and rationalise its administration.

The map can be created manually or using specialised software tools.

Cloud computing

Cloud computing is a general concept which designates the provision of services hosted on a server outside the building and accessible over the Internet.

Cloud computing enables companies to consume IT resources on demand (as they do with a public service such as electricity), avoiding them having to create and manage infrastructure internally.

IEEE committee

The International Institute of Electrical and Electronics Engineers standardisation committee, grouping the industrialists for local network products. This committee standardises the packet link protocols such as Ethernet on twisted wires and optical fibres, Wi-Fi, Bluetooth, LiFi and PLC (power Line Carrier) on low-voltage cables, etc.

ITU Committee

International Telecommunication Union standardisation committee, grouping the worldwide telecommunication operators. This committee standardises the connection protocols on real or virtual circuits used by the operators, such as the protocols of the DSL (Digital Subscriber Line) family on twisted wires, the PON (Passive Optical Network) family on mono-mode fibres, the ATM (Asynchronous Transfer Mode) family on mono-mode fibres, the DOCSIS (Data over Cable Service Interface Specification) family over mono-mode fibres and coaxial cables, etc.





Centralised distribution

Cabling with centralised distribution, consisting of distributing the sockets from a utility room or cabinet, in accordance with the cabling models ISO 11801 and FTTZ (Fibre To The Zone).

Distributed delivery

Distributed delivery cabling consists of delivering the sockets from local connection nodes spread throughout the building and/or in the activity areas and laid out near to the sockets that they distribute, in accordance with the cabling models ISO 11801 and FTTZ with Passive Consolidation Points, POL (Passive Optical LAN), FTTO (Fibre To The Office) and FTTACP (Fibre To The Active Consolidation Point).

Ecosystem

Community of equipment or software that is mutually compatible and capable of exchanging data and interacting. An ecosystem may combine equipment from several manufacturers or software publishers in a spirit of openness and interoperability.

Network access equipment

Equipment in the local network used to connect Ethernet-IP terminals of communication systems.

Core network equipment

Central equipment of the local network, providing high-bit-rate switching, in charge of controlling network resilience and routing between virtual local networks.

Handover, or roaming Wi-Fi

For wireless networks, the handover function enables equipment connected to the network to switch from one access point on the wireless network to another without losing connectivity.

This handover can be used when the equipment is moving or to balance load between different points of access to the network.

The standards IEEE 802.11F and IEEE 802.11r define the handover function for Wi-Fi networks constructed with equipment from different manufacturers (interoperability). This function is, however, generally provided in a proprietary manner with equipment from a single manufacturer.

For Wi-Fi networks, the concept of roaming is also used to designate the handover function.





For mobile telephone networks, the concept of roaming designates the roaming function. This function enables the use of a radio network belonging to a mobile operator other than one's own, for example in a zone in which one's operator does not have its own network.

HTML

HTML (Hypertext Markup Language) represents all of the tag codes inserted in a file so that it can be displayed in a web browser.

The tags tell the web browser how to present the words and images of a web page on the Internet to the user. Although each individual tag is an element in its own right, together we call them "tags". Certain elements, presented in the form of pairs, indicate the beginning and end of the display.

A formal recommendation of the World Wide Web Consortium (W3C), HTML is complied with by all browsers (Internet Explorer from Microsoft, Chrome from Google, Firefox from Mozilla and Safari from Apple), even though the display may vary from one browser to another.

HTTP

HTTP (Hypertext Transfer Protocol) is the set of rules governing the transfer of files (text, images, sound, video and other multimedia files) on the web. As soon as a user connects to the web and opens a browser, he/she is indirectly using the HTTP protocol

HTTP is an application protocol which executes on top of the TCP/IP set of protocols.

One of the concepts of the HTTP protocol includes the idea that files may contain references to other files (hence the notion of "Hypertext"), the selection of which will make other transfer requests.

All web servers contain, as well as the web pages that they serve, an HTTP daemon, meaning a program designed to wait for HTTP requests and process them upon arrival

Interoperability

Ability of a product or system to function with other existing or future products or systems, without restriction on access or use and for which the interfaces are fully known.

In contrast to the concept of "compatibility", which is a vertical concept which means that a tool can function in a given environment by complying with standards, interoperability is a transversal concept covering several systems which assume that all of the interfaces (API) are known.





IP

Computerised connection protocol (Internet Protocol) which manages the transmission of data over the Internet, based on the assignment of an identification number unique to each device connected to a network using the Internet protocol (IP address).

JSON

JSON (JavaScript Object Notation) is a readable-text data-exchange format. It is used to represent data structures and simple objects in code in a web browser.

JSON is sometimes also used in programming environments, on the server and on the workstation. JSON originated in the JavaScript programming language.

On the Internet, JavaScript uses JSON as a substitute for XML for the organisation of data. Like XML, JSON is language independent and may combine with many of them, including C++, Java, Python or Lisp.

However, in contrast to XML, JSON is only a mode of representation of data structures, unlike a full markup language. JSON documents are relatively light and their processing on the web server is therefore fast (hence its success).

Pre-connected or pre-terminated links

Fibre-optic or twisted pair cables pre-fitted with their connectors at both ends, fitted and tested by the industrialist and provided with their measuring plugs.

General Distributor Room

This is the central utility room for distributing the building's cabling. It receives the connections to external links and the central equipment for networks and equipment used in IT/communication technology. Its name standardised by ISO 11801 is the Building Distributor.

Operators' room or space

This is a room or a space in the general distributor room reserved for telecommunications operators. It collects their cable inputs and endings in a bay or a box dedicated to each operator.

Property units

Qualifies the private activity areas divided into units in the buildings, intended for several separate and independent operators.





Digital Model

Another name for the BIM, generally referring to the structured database of the BIM without any graphical representation (2D or 3D).

OSI model

The OSI (Open Systems Interconnection) model is a communication standard between network applications.

A reference model is a conceptual framework for understanding the relationships. The OSI reference model was finalised to help providers and developers create digital communications solutions and programs that interoperate and to facilitate comparisons between communication tools.

Most telecommunications operators endeavour to describe their products and services in accordance with the OSI model.

Although useful to serve as a framework for discussion and evaluation, OSI is rarely implemented because few network solutions or standard tools have all the functions associated with the layers defined as such in the model. The TCP/IP protocols which define the Internet do not perfectly correspond with the OSI model.

Developed by the representatives of the main IT and telecoms operators from 1983, the OSI model was initially intended to describe detailed characteristics of actual interfaces. Finally, the committee decided to establish a common reference model for which detailed interfaces could be developed, which, in turn, would become standards.

OSI was officially adopted as an international standard by the ISO (International Standards Organisation).

OSI Layers:

The main concept of the OSI establishes that the process of communication between two terminal points of a telecommunication network may be divided into seven separate groups of associated functions, or layers.

Each user or program that communicates is at the level of a computer capable of providing these seven functional layers. Thus, for a message exchanged between users, a flow of data transits via the layers of the source computer, reaches the network, then transits the layers of the addressee computer.

These seven functional layers are provided by a combination of applications, operating systems and drivers for the network card and network hardware, which enable a system to place a signal on a network cable or via Wi-Fi or another wireless protocol.

The seven layers of the OSI model:

- **Layer 7:** Application layer. This is the layer in which the communication partners are identified (is there someone to talk to?), that the network capacity is evaluated (does the network allow me to speak now?) and the object to be sent is created or the object to be opened is opened. (This layer is not the application itself: it is a set of services that the application must be able to use directly, even though some applications may execute functions of the application layer.)
- **Layer 6:** Presentation layer. This layer generally forms part of an operating system (OS) and is responsible for converting incoming and outgoing data





from a presentation format to another format (for example, plain text to encrypted text at one end, then return to plain text at the other end).

- **Layer 5:** Session layer. This layer manages, coordinates and terminates conversations. The services include authentication and reconnection after interruption. On the Internet, the protocols TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) provide these services to most applications.
- **Layer 4:** Transport layer. This layer manages the formation of data packets, then their delivery, and checks whether this data contains errors upon arrival. On the Internet, the TCP and UDP protocols also provide these services to most applications.
- **Layer 3:** Network layer. This layer manages the addressing and routing of data (by sending it in the right direction to the right addressee for outgoing transmissions and by receiving incoming transmissions at the packet level). For the Internet, IP is the network layer.
- **Layer 2:** Data delivery layer. This layer manages the connections on the physical network, placing the packets in the network frames. It is divided into two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). Ethernet is the main data link layer that is used.
- **Layer 1:** Physical layer. This layer is responsible for transmitting bits over the network at the electrical, optical or radio levels. It provides hardware resources for sending and receiving data on a carrier network.

TCP/IP model

The TCP/IP model is derived from ARPANET and would later become the Internet (World Wide Web).

ARPANET was originally a military project by the U.S. Army, the aim of which was to connect around a hundred universities and government facilities via telephone lines. The aim was to maintain communications at all costs after a nuclear attack.

This resulted in a network based on the routing of packets through a layer called the Internet. This layer is of the connectionless type: all packets transit independently of each other and are routed according to their content.

The TCP/IP model is therefore the model used for the Internet.

The name of the TCP/IP model is closely related to two protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). This is partly due to the fact that these two protocols are the most widely used for the Internet.

In contrast to the OSI model, there are only four layers for the TCP/IP model.

Hashed password

A hashed password is a password which uses a hash function to encrypt the passwords stored on a server. A hash function, by analogy with cooking, is a specific function which,





from input data, calculates a fingerprint that can quickly, although incompletely, identify the initial data. Only the IT client is capable of reconstituting the password.

Connection or distribution node

This is a cabling distribution point; it may be general, for a floor, for a zone or for a room.

Local connection or distribution node

Socket distribution box located in the environment close to these last; depending on the cabling model applied, it may be composed of a box of connectors for a passive consolidation point (models ISO 11801 and FTTZ), of an optical splitting box (POL model), of an optical development box (FTTO model) or of an active consolidation point (FTTACP model).

Road, utility network or overhead operator conveyance structure

Structure based on a road or utility network, composed of underground pipes routing telecommunication cables from the limit of the public domain until their entry into the building. The conveyance structures of the telecommunication operators may also be overhead.

Common parts of the building

The spaces of the building likely to be frequented by all occupants of the building, visitors, service providers in charge of safety/security, maintenance and the operation of the systems and services of the building and the public, where applicable.





Private parts of the building

Spaces of the building frequented only by the occupants for whom they are intended for their activities and by visitors authorised by these occupants.

Downlink ports

These are the ports for the network equipment used for connecting terminals.

Uplink ports

These are the network equipment ports used for interconnecting equipment on the local network.

Power over Ethernet (PoE)

PoE technology can send electrical power as well as data in a single cable. It is a function supported by network access equipment, standardised by IEEE 802.3af (15W), at (30W), bt (60W).

Protocol

In the IT field, a protocol refers to a set of rules used by network termination points to communicate during a telecommunication connection. The protocols detail the interactions between the entities that communicate.

They intervene at several levels of a telecommunication connection. For example, certain protocols govern the exchange of data at the hardware level and others at the application program level. In the standard OSI model, both ends of the exchange must recognise and observe at least one protocol at each layer of the telecommunication exchange. The protocols are often described in a sectoral or international standard.

The commonly-used Internet protocols TCP/IP are composed of several protocols:

- the TCP (Transmission Control Protocol), which uses a set of rules for exchanging messages with other Internet points at the level of the information packet;
- the IP (Internet Protocol), which uses a set of rules to send and receive messages at the level of the Internet address;
- other protocols, including HTTP and FTP (File Transfer Protocol), which define sets of rules to be used with the corresponding programs, also on the Internet.
- There are numerous other Internet protocols, such as BGP (Border Gateway Protocol) or DHCP (Dynamic Host Configuration Protocol).

The term "protocol" is borrowed from the Greek "protocollon", designating a sheet of paper glued to a manuscript volume, which describes the content.





xDSL protocols

Protocol of the Digital Subscriber Line family: ADSL (Asymmetrical Digital Subscriber Line), SDSL (Symmetrical Digital Subscriber Line) and VDSL (Very high speed Digital Subscriber Line), supported by twisted pairs of telephone wires.

Quality of Services (QoS)

Functionality for prioritising the network routing of certain traffic compared to others. The objective may be to favour telephony and the quality of the communication compared to routing an email or a file.

Smart network

The "Smart Network" is the unifying network of an R2S building, service-oriented (SOA) and using the protocol IP. It is secured and exclusively uses the Ethernet standard on the local network and the Internet standard from the exterior of the building. The hardware ecosystems, whatever their protocol, communicate on the Smart Network using APIs or web services exposed on the Smart Network and on the World Wide Web.

WAN (Wide Area Network)

This is the IP network external to the building on the public domain.

LAN (Local Area Network)

This is the Ethernet-IP network internal to the building, which may or may not have Wi-Fi terminals.

VLAN (Virtual Local Area Network)

Function that can isolate different parts of a network from each other. Standardised by IEEE 802.1q, it can identify the network to which an Ethernet frame belongs by tagging its header.

Resilience

Network function that can detect a breakdown in a link or equipment and automatically activate a process of route recalculation, to ensure continuity of service of the network in spite of the faults encountered.





REST

REST (representational state transfer) is a style of architecture for distributed hypermedia systems, enabling the production of applications for a human user or of service-oriented architectures intended for communication between machines. The REST architecture enables full decoupling of the client and the server. The user interface is separated from the storage of data. This enables both of them to develop independently (example: decoupling the three R2S layers).

RESTFull

Designates an API compatible with REST, which uses IP requests to obtain (GET), place (PUT), publish (POST) and delete (DELETE) data.

SaaS

SaaS (Software as a Service) corresponds to a mode of marketing software in which it is installed on remote servers rather than on the user's machine. Clients do not pay a usage license for a version, but freely use the online service or, more generally, pay a subscription. This model is also used for platforms (PaaS for Platform as a Service).

Information systems security

Information systems security, or more simply "IT security", is all technical, organisational, legal and human resources necessary to set up means of preventing unauthorised use, malicious use, modification or misappropriation of the information system.

In addition to the requirements of theme 4 "digital security" of R2S, a guide written by ANSSI can be consulted on the subject of the security of industrial systems.

https://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf

In particular, see appendix B.

DHCP (Dynamic Host Control Protocol) server

Function enabling the dynamic assignment of an IP address from amongst those available on the addressing plan to a terminal during session opening or during renewal of the lease on its address. A DHCP server can also obtain the IP addresses of the services present on the network (DNS, NTP...). This function avoids breakdowns caused by address duplicates that can appear when a static address is used.





DNS (Domain Name Server)

Function that can obtain the IP address that corresponds to a domain name. This function is useful, for example, for accessing a service without needing to specify its address. The service can then change addresses without disrupting access. This service may be hosted on a local or cloud-based server or may be operated.

General communication services

These are the services provided by communication systems integrated into the building for its safety/security (excluding the fire safety system), monitoring and the management of its technical systems. For the comfort and convenience of users, these systems can also be installed in common or private areas of the building.

These general communication services may be:

- Services for routing connections provided by a cabling or radio infrastructure
- Network connection services, provided by administered network equipment
- Application services, provided by communication systems and software

SPOF (Single Point Of Failure)

A Single Point Of Failure (SPOF) designates an item of equipment or a function which, if it fails, causes a total interruption of the service to which it contributes.

IT/Communication Technology system

A communication system relying on Information and Communication Technologies, whatever the subject, content and nature of the information exchanges.

Transmission Control Protocol (TCP)

TCP (Transmission Control Protocol) is one of the main transport protocols used on IP networks. It is described in detail by RFC 793 from the IETF. By using packet sequencing systems and acknowledgement of transmission/reception of data, TCP provides the various terminals on the network with essential information on the correct transmission of IP packets to their addressee.

When packets are lost on the network (which can happen when the network is saturated), TCP can resend the missing data to reconstitute the message in its entirety. TCP provides other interesting abilities, such as the option of using flow control techniques to limit the bit-rate of a connection.

It should be noted that TCP is the underlying transport protocol for HTTP, the protocol of the web, as well as most of the major Internet applications. TCP is more rarely used for real-time applications, for which another Internet transfer protocol, UDP, is often preferred.





Two-factor authentication

Two-factor authentication (2FA) or authentication in two stages, is a method by which a user can access a digital resource (a computer, an intelligent telephone or a website) after having presented two separate proofs of identity to an authentication mechanism.

Web Services

These are APIs, generally RESTfull, which are exposed on the Internet or on an Intranet, enabling communication and data exchange between applications and mixed systems in distributed environments in a synchronous or asynchronous manner.

World Wide Web

The World Wide Web is the worldwide network for the exchange and routing of data over IP (Internet Protocol), generally accessible by a web browser or by RESTfull APIs. The World Wide Web has become the worldwide network's highway for information and transactions over the Internet.

