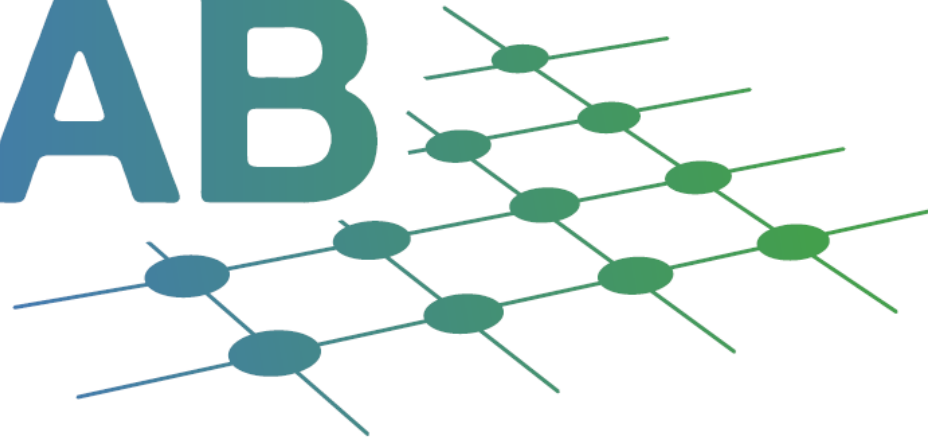


# IoT MAD LAB

UNA CIUDAD CONECTADA



MADRID

Coordinación General de la Alcaldía

Capital  
Digital



UNIVERSIDAD  
POLITÉCNICA  
DE MADRID

## IoT Laboratory of Madrid city

<https://iotmadlab.es/en/>

# Quadruple helix approach



## Public administration

- Municipal areas
- Public companies
- Regional and national governments

Demo & Validation Lab

HW Testing

## Business

- Service providers
- Technology vendors
- Urban equipment manufacturers



Training & Education

Software Integration

- Citizens
- Civil servants
- NGOs and associations

## Civil society/users



Digital Twin

City Pilots

- Universities and R&D centres
- Professional education
- Primary and High schools

## Research and Education

## Goals

- Harmonize future smart city implementations.
  - Identify open, neutral and interoperable IoT protocols and data models: technical requirements.
  - Enable interaction among municipal services.
- Boost Public-Private Innovation towards optimization and competitiveness:
  - Technological providers: devices, platforms, solutions, 5G operators.
  - Municipal services providers: management, applications, city platform.
  - Citizens: end user engagement & gamification.
  - Training and education: new skills for students and unemployed.
  - GovTech: digital government transformation.
- Urban Smart Spaces as living labs:
  - Laboratory environment.
  - University campus controlled environment.
  - Real urban environment (one in each of the 21 city districts).

Phase 0



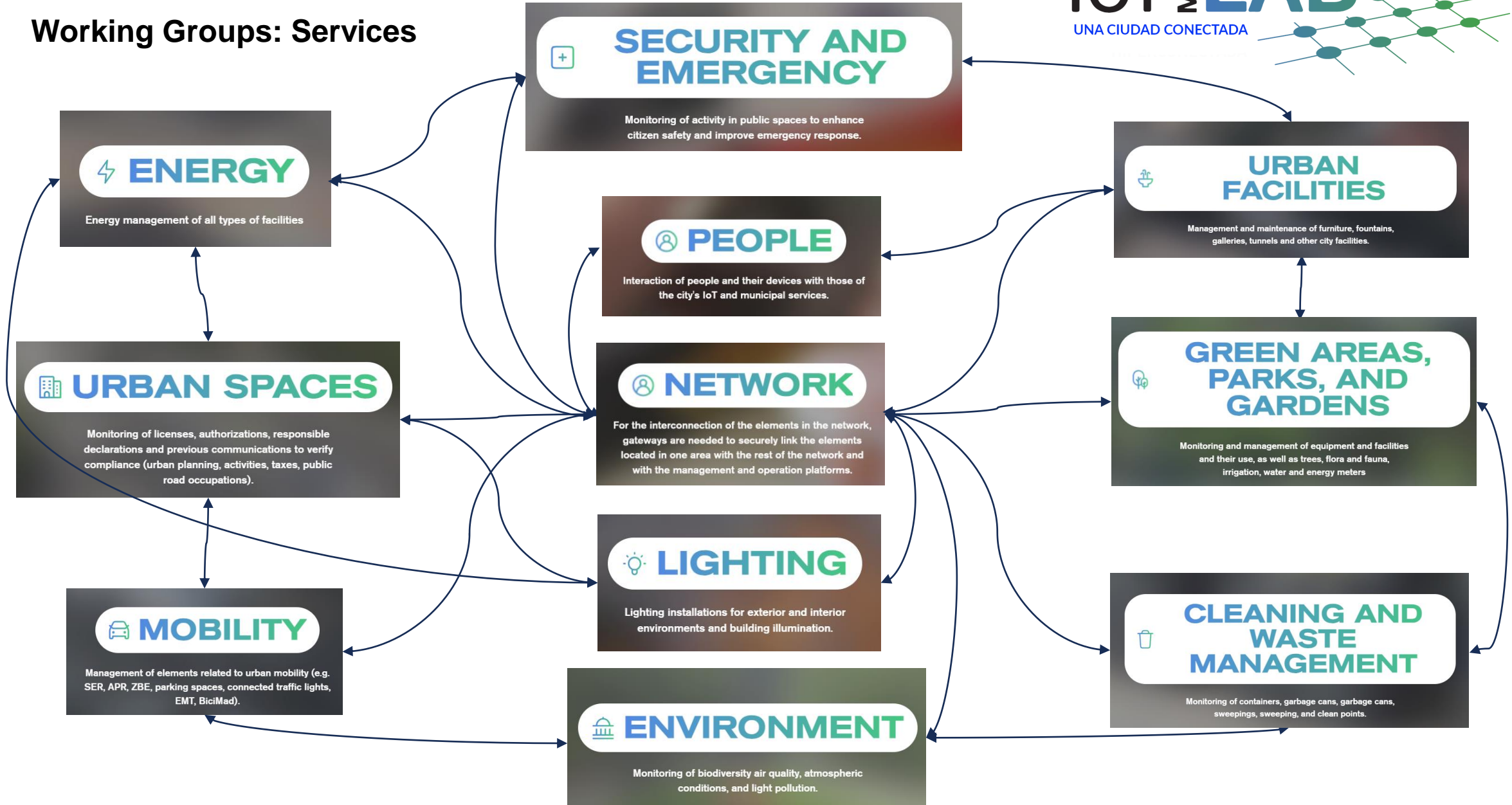
Phase 1



Phase 2

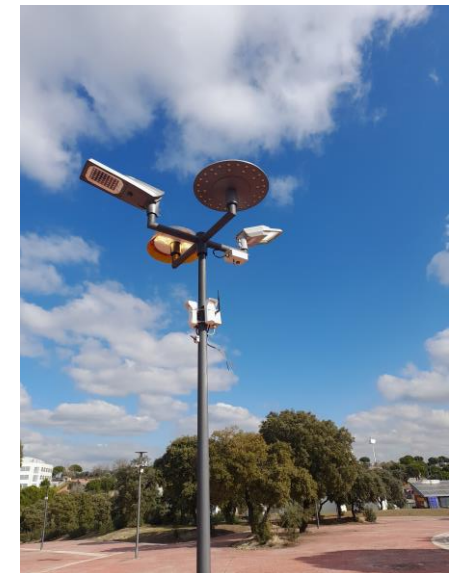


## Working Groups: Services

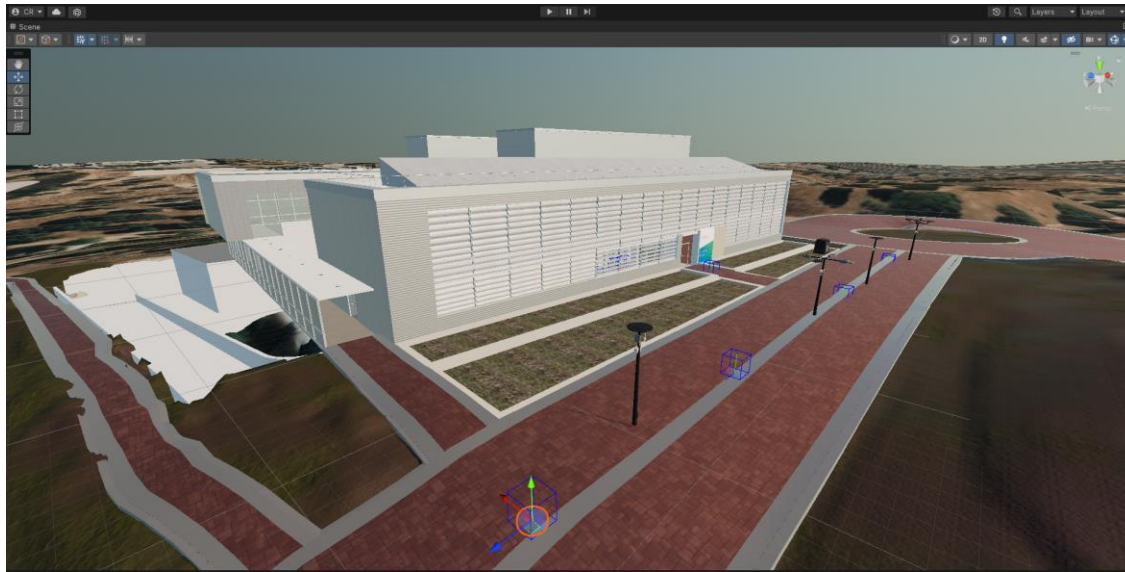




# Outdoor Laboratory: Smart space in a controlled area



# RV/AR Laboratory: Digital Twin development



## Smart Spaces in Madrid city



### SUS#1 CASA DE CAMPO

The Large Gate at the entrance to the Casa de Campo Fairgrounds has been proposed as the first deployment of a first Smart Urban Space (SUS) in the city. This demonstrator space will allow citizen interaction with the possibilities of IoT technology, and involves addressing the need for interoperability between various Municipal Areas. The objective is to achieve the best personal experience with the services provided by the City Council, and to know its future.



### SUS#2 VALDEINGÓMEZ

The Valdeingómez Technology Park is a very important industrial environment for the city of Madrid. Together with its Visitor Centre, this Smart Urban Space integrates safety in mobility, energy efficiency and environmental quality control, and opens the way to many sustainability-oriented projects.



### SUS#3 MERCAMADRID










MERCAMADRID, the largest market in Spain, feeds the city and its area of influence. Its frenetic and early morning activity takes place in a highly optimised physical space, where the application of IoT is associated with 5G SA, the autonomous vehicle (for people and goods) and energy efficiency (photovoltaic production, data market, smart consumption).





# SUS#1 Casa de Campo



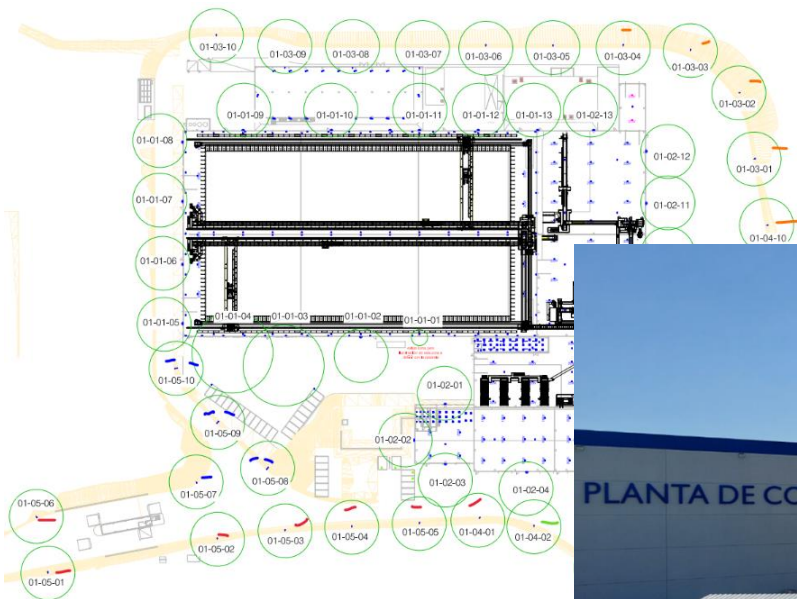
-  Outdoor exercise facilities
-  Parks and green areas
-  Mobility cameras
-  Parking areas
-  Waste bins and cans
-  VR digital twin experience
-  Street lighting fixtures
-  Citizens interaction
-  Bike lane

**Integration in a 5G corridor**

# SUS#1 Casa de Campo



# SUS#2 Valdemingomez



IDE	ZONA/ CM	LINEA ELECTRI	IDE LUMINA	MODELO LUMINARIA
01-03-01	1	3	1	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-03-02	1	3	2	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-03-03	1	3	3	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-03-04	1	3	4	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-03-05	1	3	5	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-03-06	1	3	6	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-03-07	1	3	7	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-03-08	1	3	8	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-03-09	1	3	9	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-03-10	1	3	10	LEDROAD-ST-P2- 4000K 80W - OPPLLE
01-04-01	1	4	1	ALFUM60 AE 4000K 60W - BENITO
01-04-02	1	4	2	VEKA S 4000K 53,1W - CARANDINI
01-04-03	1	4	3	VEKA S 4000K 53,1W - CARANDINI
01-04-04	1	4	4	VEKA S 4000K 53,1W - CARANDINI
01-04-05	1	4	5	VEKA S 4000K 53,1W - CARANDINI
01-04-06	1	4	6	VEKA S 4000K 53,1W - CARANDINI
01-04-07	1	4	7	VEKA S 4000K 53,1W - CARANDINI
01-04-08	1	4	8	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-04-09	1	4	9	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-04-10	1	4	10	VERA S VRS 60 ROAD III 500mA 4000K 60W - HISPALED
01-05-01	1	5	1	ALFUM60 AE 4000K 60W - BENITO
01-05-02	1	5	2	ALFUM60 AE 4000K 60W - BENITO
01-05-03	1	5	3	ALFUM60 AE 4000K 60W - BENITO
01-05-04	1	5	4	ALFUM60 AE 4000K 60W - BENITO
01-05-05	1	5	5	ALFUM60 AE 4000K 60W - BENITO
01-05-06	1	5	6	ALFUM60 AE 4000K 60W - BENITO
01-05-07	1	5	7	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-08 a	1	5	8	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-08 b	1	5	8	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-09 a	1	5	9	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-09 b	1	5	9	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-10 a	1	5	10	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC
01-05-10 b	1	5	10	TECEO 1 30 LEDS 800mA 4000K óptica 5303 77W - SOCELEC

## FABRICANTE

Denominación Social:	Schröder
Dirección física:	SCHRÉDER SOCELEC SA  Pol. Ind. El Henares - Av. Roanne 66 19180 Marchamalo (Guadalajara), España +34 9 49 32 50 80
Página WEB:	<a href="https://sp.schreder.com/es">https://sp.schreder.com/es</a>
Mail de contacto:	<a href="mailto://comercialspain@schreder.com">mailto://comercialspain@schreder.com</a>

## EQUIPO

Clasificación:	Luminaria variara > Luminarias Post-top
Denominación:	IZYLUM
Referencia comercial:	
Versión / fecha de comercialización:	
Imagen	

URL del producto: <https://sp.schreder.com/es/productos/iluminacion-led-exterior-izylum>

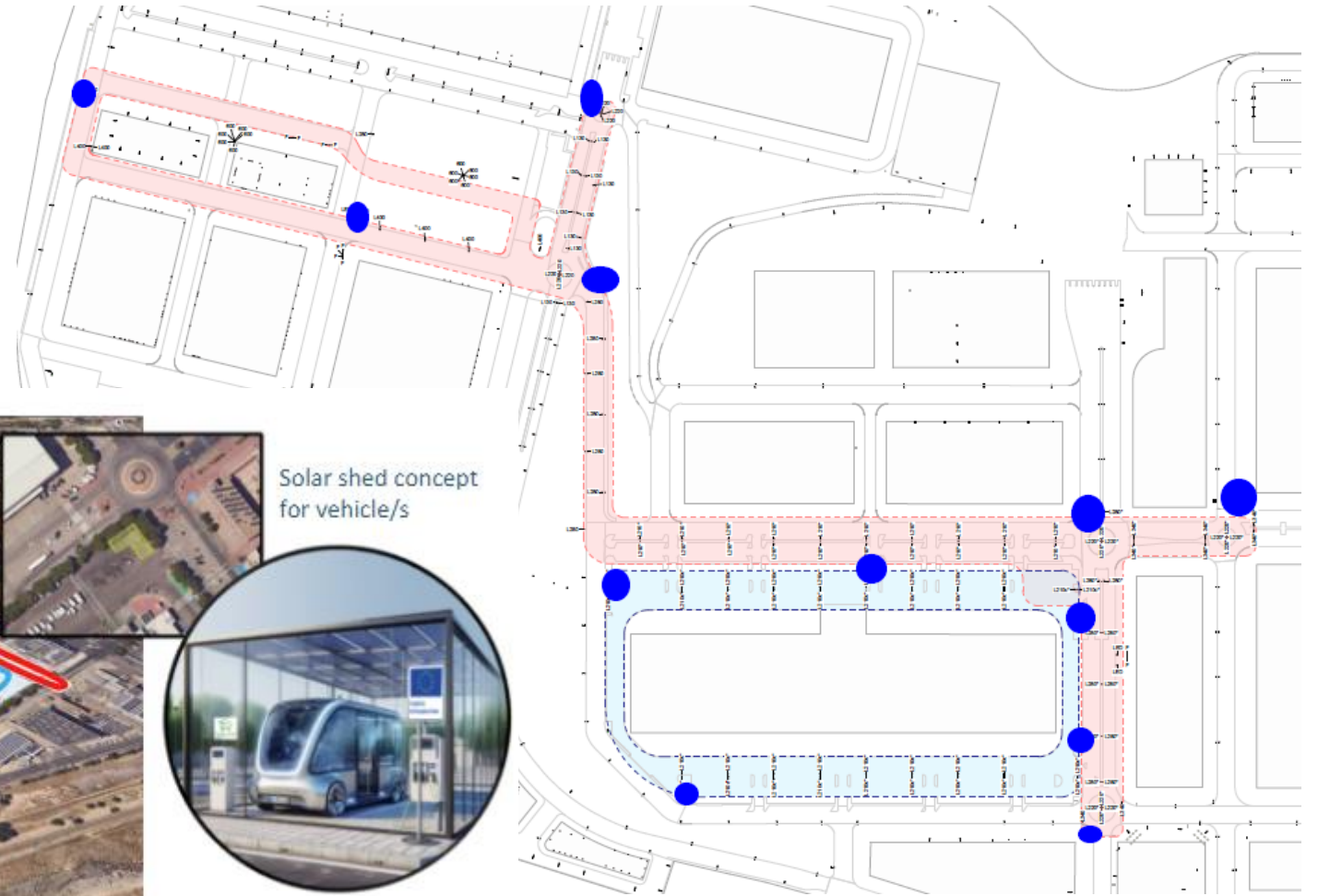
Características: Altura recomendada para la instalación: 4 – 15 m.  
  
Temperatura de funcionamiento: -40°C a +55°C.  
  
Módulo de LEDs: 40 LEDs.

Sensores: Como miembro fundador del consorcio Zhaga, Schröder ha participado en la creación del programa de certificación Zhaga-D4i y en la iniciativa de este grupo para estandarizar un ecosistema interoperable.

## ANEXO I: CHECKLIST LUMINARIA

Conector Zhaga superior	Sí
Conector Zhaga inferior	Sí
Protocolo Dali4	Sí
Alimentación	220 – 240 V
Control con nodo IoT	Sí
Control con sensor PIR	Sí
Descubrimiento en Plataforma IoT	Sí
Apertura sin herramientas	Sí

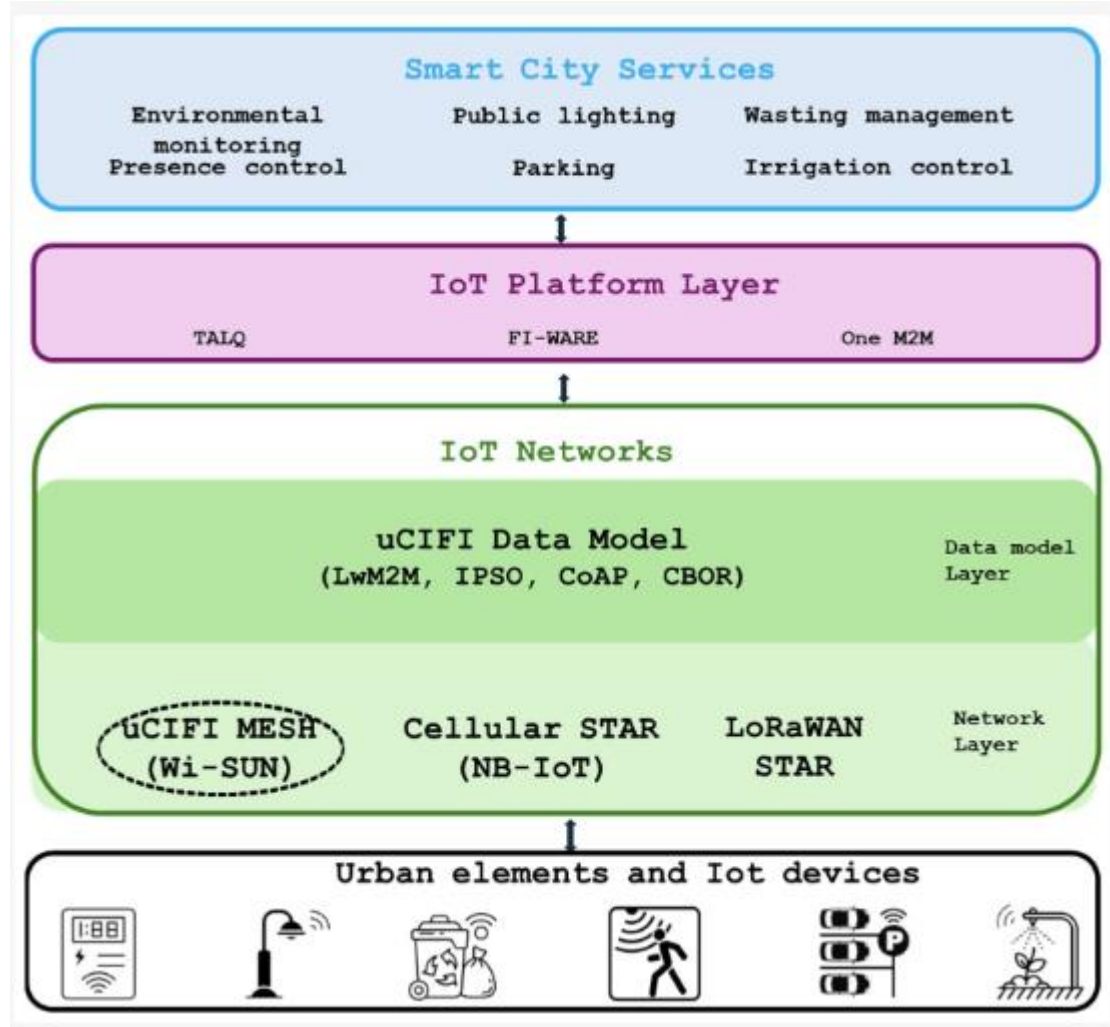
# SUS#3 MercaMadrid



Solar shed concept for vehicle/s



# IoT Network Reference Architecture



Object Name	ID	Instances	Object URN
Temperature Sensor	3303	Multiple	urn:oma:lwm2m:ext:3303

Resource	ID	Oper.	Mandatory	Type	Units	Description
Sensor Value	5700	R	Mandatory	Float	Defined by "Units" resource	Current measured sensor value
Min Measured Value	5601	R	Optional	Float	Defined by "Units" resource	The minimum value measured by the sensor since power ON
Max Measured Value	5602	R	Optional	Float	Defined by "Units" resource	The maximum value measured by the sensor since power ON
Min Range Value	5603	R	Optional	Float	Defined by "Units" resource	The minimum value that can be measured
Max Range Value	5604	R	Optional	Float	Defined by "Units" resource	The maximum value that can be measured
Sensor Units	5701	R	Optional	String		Measurement units definition e.g. "Cel" for celsius
Reset Min and Max Measured Values	5605	E	Optional	String		Reset the min and max measured values to current value

**Collaborative work:** between Madrid City (CCMAD) and UPM (GB2S and RSTI R&I Groups).

**Global focus:** cybersecurity threats in all IoT layers within a Smart City.

**Real implementation:** theoretical analysis and experimental validation in EUIs.

IoT devices and communications



5G environments



Cyber-situational awareness



Centro de  
Ciberseguridad  
Ayuntamiento  
de Madrid



## Cybersecurity for IoT devices and communications



Theoretical analysis of IoT ecosystems and within the Smart City paradigm



Development of evaluation methodologies



Experimental testing and validation



Vulnerability analysis



## Cybersecurity for 5G environments



5G Security architecture analysis



Study on threats and security challenges in 5G



Virtualized security testing infrastructure design



Laboratory threat testing



## Cyber-situational awareness for Smart Cities



Analysis of risk management methodologies



Design of control console for assets monitorization



Intrusion detection based on AI



AI integration in decision-support systems

- **Lightweight cryptography** (extreme conditions)
- **Suitable ciphers selection:**
  - ASCON -new standard- (symmetric)
  - Elliptic Curves (asymmetric)
- **Security analysis:**
  - Conventional cryptological attacks
  - Side channel attacks

## Requirements Checklist

### 2.1. Componentes del dispositivo

- 2.1.1. Unidades de proceso
- 2.1.2. Memoria
- 2.1.3. Firmware
- 2.1.4. Servicios de intercambio de datos

### 2.2. Interfaces del dispositivo

- 2.2.1. Interfaces internas
- 2.2.2. Interfaces físicas (M2M)
- 2.2.3. Interfaces inalámbricas (M2M)
- 2.2.4. Interfaces de usuario (H2M)

### 2.3. Descripción general del modelo

## 3. Listado de requisitos

### 3.1. Requisitos técnicos

- 3.1.1. Identidad de dispositivos y sistemas IoT
- 3.1.2. Configuración de dispositivos IoT
- 3.1.3. Almacenamiento en la memoria del dispositivo
- 3.1.4. Interfaces de comunicaciones
- 3.1.5. Software, firmware y unidades de proceso
- 3.1.6. Servicios de intercambio de datos

### 3.2. Requisitos no técnicos

- 3.2.1. Documentación
- 3.2.2. Procesos de desarrollo seguros
- 3.2.3. Gestión de vulnerabilidades
- 3.2.4. Actualizaciones
- 3.2.5. Privacidad
- 3.2.6. Incumplimiento de requisitos

## 4. Checklist

### 4.1. Requisitos técnicos

- 4.1.1. Identidad de dispositivos y sistemas IoT
- 4.1.2. Configuración de dispositivos
- 4.1.3. Almacenamiento en la memoria del dispositivo
- 4.1.4. Interfaces de comunicaciones
- 4.1.5. Software, firmware y unidades de proceso
- 4.1.6. Servicios de intercambio de datos

### 4.2. Requisitos no técnicos

- 4.2.1. Documentación
- 4.2.2. Procesos de desarrollo seguros

### 3.1.5. Software, firmware y unidades de proceso

Id	Requisito	Descripción
1.5.1	Disponibilidad de funcionalidades y software no necesario	En general se deberían deshabilitar o eliminar todas las funcionalidades o software no necesario para el funcionamiento del dispositivo.
1.5.2	Privilegios mínimos	Los dispositivos deben ejecutarse con el mínimo nivel de privilegio posible para su funcionamiento.
1.5.3	Arranque seguro	El dispositivo debe contar con mecanismos de arranque seguro.
1.5.4	Protección ante <u>debugging</u>	Los dispositivos deben estar protegidos ante el uso no autorizado de funciones de prueba o <u>debugging</u> .
1.5.5	Gestión de la configuración y actualizaciones	El dispositivo debe contar con un sistema de gestión de actualizaciones para evitar el uso de software desactualizado en sus interfaces.
1.5.6	Verificación de la actualización de software	El dispositivo debe contar con procesos para asegurar la autenticidad e integridad de las actualizaciones de software y firmware.
1.5.7	Automatización de actualizaciones	Se deberían emplear métodos automáticos periódicos para la actualización del software o firmware. Un usuario autorizado debería ser capaz de deshabilitar, posponer o habilitar las actualizaciones.

### 3.1.2. Configuración de dispositivos IoT

	Requisito	Descripción
2.1	Control de acceso para configuración	El dispositivo cuenta con mecanismos de autenticación y autorización para el acceso que permita realizar cambios de configuración (incluyendo parámetros críticos de seguridad) a través de alguna interfaz (física, inalámbrica, de usuario).
2.2	Configuración entre dispositivos	Si un dispositivo puede configurar la seguridad de otro dispositivo en el entorno <u>IoT</u> , debe poderse demostrar que los cambios de configuración se aplican en el otro dispositivo.
2.3	Unicidad de parámetros críticos de seguridad	Los parámetros críticos de seguridad, como contraseñas, identidades, etc., deben ser únicos por dispositivo, generados en su fabricación y no devueltos a valores genéricos universales.
2.4	Obtención de parámetros críticos de seguridad	Los parámetros críticos de seguridad, como contraseñas, identidades, etc. no deben ser fáciles de obtener mediante procesos automáticos o información pública.
2.5	Seguridad de los parámetros críticos	Los parámetros críticos de seguridad deben adaptarse a criterio de seguridad como longitud, complejidad, proceso de generación de claves, procesos de gestión y almacenamientos seguros.



Industry and International support



---

## Stakeholders benefits



**Local government:** IoT digital infrastructure harmonization.

**Technological vendors:** alignment with a technical definition.

**Service providers:** management capacity and competitiveness boost.

**Municipal areas:** provider agnostic (higher competency and transparency).

**Research and academia:** new collaboration and funding opportunities.

**Citizens:** engagement and co-creation enabling.

**Education:** digital and future skill courses and capacities.

**International community:** network of IoT living labs.

## Contact

**Fernando Alvarez**

Digital Office - Madrid City Council

**Asuncion Santamaria**

CEDINT - Universidad Politecnica de Madrid

**Guillermo del Campo**

CEDINT - Universidad Politecnica de Madrid

 <https://iotmadlab.es/en/>

 <https://www.linkedin.com/company/iotmadlab/>

