SAT-ICS para la monitorización de Smart Cities

Contexto

El término Smart City o ciudad inteligente es usado para referirse a ciudades basadas en un desarrollo sostenible, que usan las diferentes tecnologías de la información y comunicación para la gestión y prestación de sus diferentes servicios. En el contexto de una ciudad inteligente, los sistemas de control industrial y demás sistemas IIoT, juegan un papel esencial para asegurar el funcionamiento eficiente y seguro de las diversas infraestructuras y servicios que la hacen posible. Estos sistemas integran y automatizan una amplia gama de procesos para mejorar la calidad de vida de los ciudadanos, permiten la optimización de los recursos y ayudan a reducir el impacto ambiental, entre otras funcionalidades. Sin embargo, la introducción de estos sistemas ha abierto también una puerta a riesgos que debemos ser capaces de identificar y gestionar, evitando cualquier posible impacto grave en la seguridad de los ciudadanos.

Dispositivos implicados

Existe una gran diversidad de dispositivos que pueden interactuar en el entorno de una ciudad inteligente. Es posible encontrar tanto dispositivos OT tradicionales (sensores y controladores) como otros dispositivos IoT o IIoT. Existen multitud de tipologías de despliegue de dispositivos, generalmente, este parque diverso de dispositivos se conecta y gestiona de diferentes formas como; puertas de enlace inalámbricas, pasarelas serie, 4G/5G, fibra, ethernet, etc. Estos elementos actuarían como elementos para, por ejemplo, el filtrado de datos, gestión de dispositivos, control de acceso y comunicación compartida con redes y aplicaciones.

Estos dispositivos se pueden desplegar tanto con acceso a la propia red del Ayuntamiento, como pertenecer a terceros y que la comunicación pueda realizarse directamente o mediante concentradores, de forma inalámbrica o cableada. La comunicación de estos dispositivos también puede extenderse hacia la nube. Este entorno cloud se encarga de consolidar y analizar datos, procesar eventos, proporcionar acceso a los datos a las distintas aplicaciones y llevar a cabo

diversas funciones adicionales. No existe una única arquitectura que represente todos los tipos de infraestructuras desplegadas y modos de explotación posibles dentro del sector, por lo que los puntos de red monitorizados dependen de la realidad de cada caso.

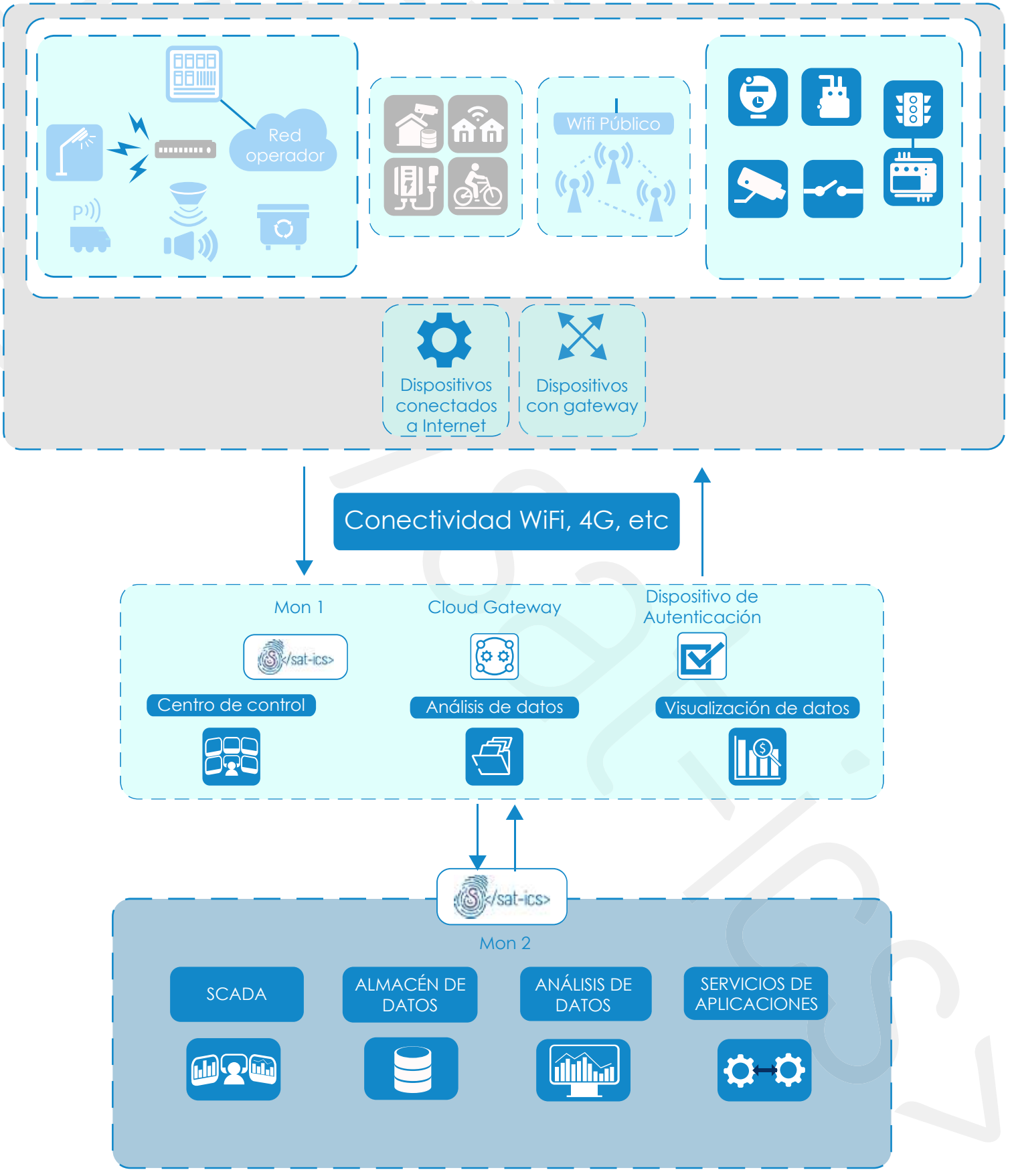
Aunque esta variedad de tipologías de despliegue dificulta la monitorización, es posible analizar el tráfico en los puntos en los que estos sistemas se interconectan hacia los sistemas centrales y bases de datos. Estas comunicaciones requieren de una supervisión y control para evitar cualquier posible abuso.

¿Por qué SAT-ICS?

El sistema alerta temprana ICS (SAT-ICS), permite la detección a tiempo real de las amenazas e incidentes en el tráfico de las redes asociadas a estos dispositivos, e incluso una rápida reacción ante un posible incidente de seguridad.

Monitorización de ciudades inteligentes centralizadas

Como se puede observar en la arquitectura, tenemos 3 zonas diferenciadas, y dos opciones de monitorización. En el caso de que se pueda acceder al cloud gateway, porque esté en red local, se podrá monitorizar (Mon 1), en caso contrario tendremos solo un punto de monitorización en nuestra red local (Mon 2).


Red operador
Wifi Público
Dispositivos conectados a Internet
Dispositivos con gateway
Conectividad WiFi, 4G, etc
Mon 1
Cloud Gateway
Dispositivo de Autenticación
Centro de control
Análisis de datos
Visualización de datos
Mon 2
SCADA
ALMACÉN DE DATOS
ANÁLISIS DE DATOS
SERVICIOS DE APLICACIONES

¿Qué aporta a estos sistemas?

Detección de ataques e incidentes:

Con generación de alertas basadas no sólo en el análisis del tráfico de protocolos típicamente TI, sino también del tráfico en los protocolos específicos empleados en la comunicación entre controladores PLC, RTU, instrumentación, servidores SCADA, sistemas de seguridad, equipamiento IoT, etc.

Inventario y mapa de activos:

Para el apoyo a la gestión de las redes de dispositivos ciberfísicos a partir de la identificación pasiva de activos y el análisis del flujo de comunicaciones entre redes y conexiones a Internet.

Detección en base a anomalías:

El Sistema de Alerta Temprana en Sistemas de control Industrial (SAT-ICS) del CCN-CERT permite la detección en tiempo real de las amenazas e incidentes en el tráfico de las redes asociadas a estos dispositivos. Además, favorece una respuesta rápida ante un posible incidente de seguridad; algo fundamental en unas infraestructuras que pertenecen a un sector considerado como crítico.

Correlación:

El sistema central no solo detecta incidentes importantes de forma individual, sino que localiza eventos mucho más complejos que pueden involucrar a distintos organismos. Adicionalmente, proporciona acceso al mayor conjunto de reglas de detección que permite la detección de un mayor número de amenazas actualizadas de manera continua y enfocada para este tipo de entornos.

Elaboración de casos de uso específicos:

Es posible generar alertas específicas del tráfico de red para situaciones de riesgo definidas por el propio organismo y de las cuales se quisiera tener constancia. Para esto CCN-CERT requerirá que este facilite la información necesaria para poder configurar las reglas de detección apropiadas.

Informes estadísticos y soporte a la resolución de incidentes:

Información de gran valor para los responsables de seguridad de estos sistemas, que pueden ver en tiempo real el estado de su red y acceder a diversos informes estadísticos.