XLIV Jornadas de Automática 2023

https://jautomatica.es

# Control de acceso remoto a redes industriales

Díaz-Cacho, Miguel.[a,*], Chaves, Andre.[b], Pereira, Alejandro.[c]

[a] *Dept. Ing. Sistemas y Automatica, Universidade de Vigo*

[b] *Instituto Politecnico de Bragança, Bragança, Portugal*

[c] *Departamento de Diseño en la Ingeniería, Universidade de Vigo*

**To cite this article:** Diaz-Cacho, Miguel, Chaves, André, Pereira, Alejandro. 2023. MQTT as control protocol for remote acces to industrial networks.
XLIV Jornadas de Automática, 795-800. https://doi.org/10.17979/spudc.9788497498609.795

**Resumen**

El acceso remoto a redes industriales es una de las contribuciones que la Industria 4.0 ha popularizado al habilitarse la integración de las tecnologías TCP/IP en las redes OT y poder realizarse dicho acceso a través de la red pública Internet. De esa forma se posibilita ejecutar operaciones de mantenimiento de forma remota con mejoras en recursos y costes respecto a las opciones previas. No obstante, este acceso hace que los riesgos de seguridad aumenten al abrirse una nueva e importante vulnerabilidad y existir la posibilidad de acceso desde cualquier equipo conectado a Internet. Para poder gestionar de forma eficiente estos accesos remotos, este trabajo propone el uso del protocolo industrial de telemetría MQTT en el intercambio de comandos de control de acceso entre las partes implicadas. Ello permite una modalidad de acceso oportunista que disminuye cuantitivamente hasta en cuatro los niveles de seguridad requeridos según la norma IEC62443. La propuesta incluye una topología basada en tres elementos, el *Ancla*, el *UNet* y el *Nauta* y en tres servicios ofrecidos en formato Open-Source, el servicio de redirección de puertos, el servicio de acceso y el servicio de control de acceso.

*Palabras clave:* Ciberseguridad industrial, MQTT, Acceso remoto, Red Privada Virtual, Mantenimiento 4.0.

**MQTT as control protocol for remote acces to industrial networks.**

**Abstract**

Remote access to industrial networks is one of the contributions that Industry 4.0 has popularized by enabling integration of TCP/IP technologies in OT networks and, therefore, to make industrial networks reachable using the public Internet. Remote maintenance is one of the great beneficiaries of this functionality. However, this access increases the security risks because a new and important vulnerability is opened by the possibility of remote access from any computer connected to the Internet. In order to efficiently manage these remote accesses, this paper proposes the use of the industrial telemetry protocol MQTT in the exchange of access control commands between the involved devices. This allows an opportunistic access modality that quantitatively reduces the security levels required by the IEC62443 standard by up to four. The proposal includes a topology based on three elements, the *Anchor*, the *UNet* and the *Nauta* and on three different services offered in Open-Source format; the port-redirection service, the access service and the access control service.

*Keywords:* Industrial Cibersecurity, MQTT, Remote Access, Virtual Private Network, Maintenance 4.0.

*Autor para correspondencia: mcacho@uvigo.es

## 1. Introducción

En el proceso de despliegue de la Industria 4.0, se ha generado un aumento significativo de los riesgos en ciberseguridad, hasta el punto de que este factor está siendo uno de los principales obstáculos para una adopción definitiva de la misma. Una de las funcionalidades mas sensible de la Industria 4.0 en el ámbito de la ciberseguridad es el acceso remoto a redes industriales para la realización de labores de mantenimiento, al ofrecer accesos externos a los dispositivos de la red, acceso que antes no existía. Según (Cisco Cybersecurity Team, 2018), las debilidades en procedimientos seguros en entornos industriales tras la implantación de la Industria 4.0 son una de las principales fuentes de explotación de vulnerabilidades para obtener acceso a los sistemas de control y producción industriales.

No obstante, dicho acceso de forma remota es útil para la realización de labores de mantenimiento. Por ello, varios productos comerciales ofrecen soluciones en las que en las redes industriales se instalan unos dispositivos, en general llamados *pasarelas*, que habilitan una conectividad desde el exterior hacia las mismas sin necesidad de una implicación de los departamentos de tecnologías de la información (IT) para su consecución. Un ejemplo conocido de esos productos es *Secomea* (Secomea Team, 2022).

Este trabajo presenta una solución alternativa utilizando tecnologías abiertas y conocidas por el sector de tecnologías de la operación (OT). La solución propuesta ofrece una conectividad hacia las redes industriales de caracter oportunista, de forma que la disponibilidad del acceso remoto se realiza bajo demanda del personal de mantenimiento que busque acceder a la red industrial. Ello aumenta significativamente la seguridad mediante una reducción cuantitativa de la probabilidad de ataque al disminuir la ventana temporal en la que el ataque es posible. Según los procedimientos de la norma IEC62443, cuantitativamente implica una disminución de 4 niveles en el análisis de riesgos (Diaz-Cacho et al., 2019).

## 2. Acceso remoto a redes industriales

El acceso remoto consiste en la posibilidad de acceso digital a una red industrial con tecnología Ethernet desde una red externa a la organización. El término "remoto" es empleado desde el punto de vista de la red industrial. La red industrial está integrada en una intranet y protegida por uno o varios dispositivos cortafuegos (*firewalls*). La configuración mas común de los *firewalls* permite la salida controlada de la red industrial hacia el exterior (Internet) para el envío puntual de información o la actualización de firmware, y en cambio bloquea cualquier acceso desde Internet a la misma.

### *2.1. Topología básica de acceso remoto a redes industriales*

La Figura 1 muestra una topología básica de acceso remoto con una propuesta de nomenclatura de los distintos elementos implicados.

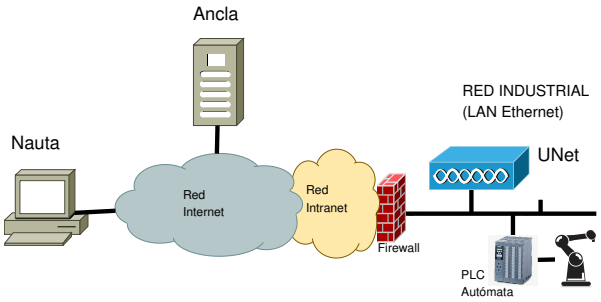


Figure 1: Topología básica de acceso remoto.

La nomenclatura utilizada permite una identificación intuitiva de la funcionalidad de los dispositivos. Los principales dispositivos son el *Nauta*, el *Ancla* y el *UNet*.

**Nauta** equipo remoto operado por personal especializado desde el que se realiza el acceso a la red industrial para las operaciones de mantenimiento.

**UNet** acrónimo de UnderNet, o "TrasLaRed": equipo al que se accede remotamente desde el *Nauta* y que está físicamente en la red industrial. Este equipo contiene los servicios necesarios para servir de pasarela entre el *Nauta* y la red industrial.

**Ancla** equipo visible en Internet que sirve de "punto de apoyo" para el *Nauta* y el *UNet*. Este equipo debe ser accesible desde el *Nauta* y desde el *UNet*. No todas las estrategias de acceso remoto precisan de un *Ancla*.

### *2.2. Estrategias de acceso remoto a redes industriales*

Las redes industriales incluyen desde equipos informáticos hasta robots industriales controlados por autómatas o PLCs. Los PLCs disponen de programas que realizan el control de los robots y estos programas se actualizan, modifican o corrigen en el marco de labores de mantenimiento. El acceso a los programas suele hacerse en la propia red local del autómata mediante los entornos de programación específicos instalados en equipos llamados genéricamente *programadores*.

Disponer de un acceso remoto con niveles de seguridad reconocidos en el IEC62443 a una red industrial es muy útil para la ingeniería de mantenimiento, evitando numerosos desplazamientos a las instalaciones.

Existen 2 estrategias fundamentales:

**Acceso mediante escritorio remoto** (VNC, RemoteDesktop, TerminalServer, etc) al *UNet*, que dispondría de las herramientas necesarias para la ejecución de las acciones sobre el dispositivo a mantener. El principal inconveniente es la necesidad de tener un *UNet* completamente equipado en cada una de las redes industriales a las que acceder de forma remota. Como ejemplo, en una red industrial PROFINET, el *UNet* (que sería servidor VNC o TerminalServer) requeriría tener instalada una instancia TIA-Portal suficiente para la operación, configuración y programación de los PLCs. En el caso de varias redes industriales remotas, habría que disponer de instancias TIA-Portal en cada

una de ellas, con el consiguiente coste en licencias y requerimientos hardware para su funcionamiento.

**Acceso mediante *VPN* (Lin et al., 2000)** donde el *UNet* llevaría el servidor *VPN* y el *Nauta* el cliente *VPN*. El *Nauta* entraría dentro de la red industrial a través del *UNet* como si formase parte de ella, y por tanto sería el *Nauta* el que tendría las herramientas para realizar las acciones de mantenimiento. En el ejemplo de acceso a una red PROFINET, la instancia de TIA-Portal estaría instalada en el *Nauta*, independientemente de la red industrial remota a la que se pudiese acceder. Por ello, el equipamiento necesario para el *UNet* es muy básico, limitándose a la herramienta *VPN*, que además puede ser abierta y de uso libre como OpenVPN (OpenVPN Team, 2022) o WireGuard (Wireguard Team, 2022) o utilizar una solución comercial como Secomea. Eventualmente, podría ser suficiente con un acceso *SSH* si el *UNet* puede realizar las acciones desde línea de comandos.

Estas estrategias han de aplicarse por parte del personal técnico de la red industrial partiendo de dos situaciones habituales :

- Es posible dar acceso remoto al *UNet* mediante reglas DNAT (Destination Network Address Translation) (Jennings and Audet, 2007) del *firewall*. Es el personal IT el responsable de su ejecución y el personal de mantenimiento dependería de ello. Para que esta solución sea segura es necesario activar/desactivar el acceso externo mediante cambios en las reglas del *firewall* cada vez que se quiera habilitar el acceso externo a la red industrial. Implica además crear reglas con limitaciones en origen y destino de los flujos de datos. Por contra, esta situación no necesita la existencia de un *Ancla*.
- No es posible (o muy complicado) dar acceso remoto al *UNet* desde Internet. Esta situación obligaría a disponer de un *Ancla*, pues sirve como nexo de comunicación entre el *Nauta* y el *UNet* que de otra forma no es posible. Esta comunicación entre el *Nauta* y el *UNet* se realiza con técnicas de redirección de puertos en el *Ancla*.

Este trabajo considera la situación en la que no es posible dar acceso remoto al *UNet* desde Internet. Es la mas habitual para el personal encargado de OT o cuando la red industrial está integrada en una topología de varias redes locales encapsuladas unas en otras en las que existen varios *firewalls* en cascada.

## 3. Plataforma de control de acceso remoto

La plataforma de control de acceso remoto propuesta incluye todos los componentes hardware y software para la realización de las operaciones de mantenimiento. Esta plataforma consta de los tres elementos presentados en la sección 2.1, el *Nauta*, el *Ancla* y el *UNet*. El *Ancla* y el *UNet* permiten la habilitación de conexiones de forma transparente y segura a las redes industriales desde cualquier lugar donde haya un equipo de usuario (*Nauta*) para la realización de tareas de mantenimiento y facilitar los análisis preventivo y predictivo. Esta plataforma dispone de 3 servicios: i) el *servicio de redirección de puertos*, ii) el *servicio de acceso* y iii) el *servicio de control de acceso*.

### *3.1. Servicio de redirección de puertos*

La topología de acceso propuesta que utiliza un *Ancla* como dispositivo intermedio hace uso de las herramientas de redirección de puertos remotos incluidas en el protocolo secure shell (*SSH*) (Ylonen and Lonvick, 2006). Esta redirección de puertos se presenta como un servicio ofrecido por el *Ancla* y la aplicación cliente será ejecutada en el *UNet*. El proceso de redirección remota de puertos puede verse en la Figura 2.

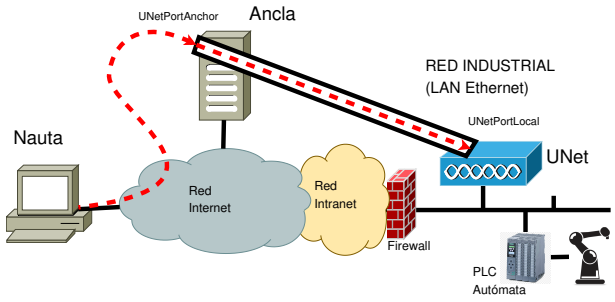


Figure 2: Topología de acceso

En dicha figura se muestra cómo el *UNet* establece una conexión *SSH* con el *Ancla* en la que busca exclusivamente redireccionar el puerto TCP “UNetPortAnchor” del *Ancla* hacia el puerto TCP “UNetPortLocal” del *UNet*. El protocolo *SSH* lo permite en su sección “Port-forwarding”, donde se permite la redirección (forwarding) de un puerto del equipo remoto hacia otro puerto del equipo local. La sintaxis de dicha redirección utilizando “OpenSSH” aparece en el código de consola 1,

Code 1: UNet. *SSH* port local redirection.

```
userUnet@UNet:~ $ ssh -f -N -p <AnchorPort> -R 0.0.0.0:<↩
    UNetPortAnchor>:localhost:<UNetPortLocal> <AnchorUser↩
    >@<AnchorIP>
```

donde “<AnchorPort>” sería el puerto del servicio *sshd* del *Ancla* y “<UNetPortAnchor>” el puerto abierto en el *Ancla* para la redirección al puerto “<UNetPortLocal>”. En la Tabla 3 se describen, entre otros, estos parámetros. El usuario “<AnchorUser>” debe de tener autorización de redirección en el *Ancla*, identificado como “<AnchorIP>” o “<AnchorDNS>”; se recomienda implementar esa autorización mediante el sistema de certificados para evitar tener que teclear su clave de acceso cada vez que se desee activar la redirección.

Como ejemplo, si en el puerto “<UNetPortLocal>” del *UNet* está escuchando el servicio *sshd*, desde el *Nauta* habría que ejecutar

Code 2: Nauta. Acceso a la consola *SSH* del *UNet*.

```
userNauta@Nauta:~ $ ssh -p <UNetPortAnchor> userUnet@Ancla
userUnet@UNet:~ $
```

para acceder a la consola *ssh* del *UNet*. Puede verse que a pesar de establecer conexión al *Ancla*, esta se realiza con el usuario ”userUnet“ (”userUnet@Ancla“), pues el puerto ”<UNetPortAnchor>“ del *Ancla* está redirigido al puerto ”<UNetPortLocal>“ del *UNet* (en este caso el puerto de

escucha del servicio "*sshd*"). Para establecer una conexión *VPN*, el puerto "<UNetPortLocal>" sería el puerto TCP/UDP en el que escuchase el servicio "*vpnd*" del *UNet*.

### 3.2. Servicios de acceso

El conjunto de *servicios de acceso remoto* engloba las herramientas que permiten acceder digitalmente de forma remota a las redes internas, descritas en la sección 2.2. Este trabajo se centra en el protocolo *SSH* y las técnicas de redes privadas virtuales *VPN* representados por los servicios "*sshd*" y "*vpnd*". Estos servicios deberán estar instalados en el *UNet*, y las aplicaciones cliente de los mismos deberán estar instaladas en el *Nauta*.

### 3.3. Servicio de control de acceso remoto mediante MQTTs

El *servicio de control de acceso remoto* es el entorno de control de los servicios de acceso. Este entorno permite monitorizar y activar/desactivar los servicios de acceso *sshd* y *vpnd*.

El entorno operativo del *servicio de control de acceso remoto* es proporcionado por una consola de control llamada *dashboard* a la que se accede desde el *Nauta*, y desde la cual se controlan los *servicios de acceso* y se monitoriza el estado de los mismos.

Para el intercambio de la información de control y monitorización entre los 3 elementos topológicos implicados se utiliza el protocolo MQTT en su versión segura (MQTTs). El intercambio de información se realiza en dos flujos de datos, el *flujo de control* y el *flujo de monitorización*. En el flujo de control se transmiten las órdenes de activación/desactivación de los servicios de redirección (Sección 3.1) y de acceso (Sección 3.2), y en el flujo de monitorización se informa del estado de dichos servicios y otros parámetros.

#### 3.3.1. Control MQTTs

MQTT es un protocolo orientado al intercambio de datos de telemetría para entornos SCADA. Utiliza un modelo de publicación/suscripción en espacios de memoria llamados *topics* en un gestor central llamado *broker*. De esa forma no es necesario que el dispositivo que publica datos en un *topic* y el dispositivo que se suscribe a ese *topic* para recibir esos datos tengan comunicación directa entre ellos, bastando con tener ambos comunicación con el *broker*. Esta característica hace que el *broker* MQTT pueda estar instalado en el *Ancla*, visible tanto por el *Nauta* como por el *UNet* (Figuras 3 y 4).

El control MQTTs está basado en dos flujos de datos, que se intercambian en dos *topics* diferentes del *broker* MQTT:

- Flujo de control (topic: "control"). Figura 3.
  - Publicación de las acciones para la activación/desactivación de los servicios que habilitan el acceso remoto, es decir, el servicio de redirección de puertos y el servicio de acceso al *UNet* y los parámetros asociados (Tabla 3). En la Figura 3, el *Nauta* se conecta a la interfaz del *dashboard* (flujo 1a) y publica en el topic "control" la activación/desactivación de un servicio con sus parámetros (flujo 2a).
  - Suscripción del *UNet* al topic "control" y recepción de las órdenes de acciones a realizar con sus parámetros (flujo 3a de la Figura 3). El *UNet* estará ejecutando un servicio de recepción de mensajes de control (suscripción al topic "control") y ejecutará la suite de scripts y comandos para la activación o desactivación de los servicios de redirección y acceso (flujo 4a). Si la acción era de activación, el *Nauta* realiza el acceso remoto al *UNet* (flujo 5a), y por tanto a la red industrial.

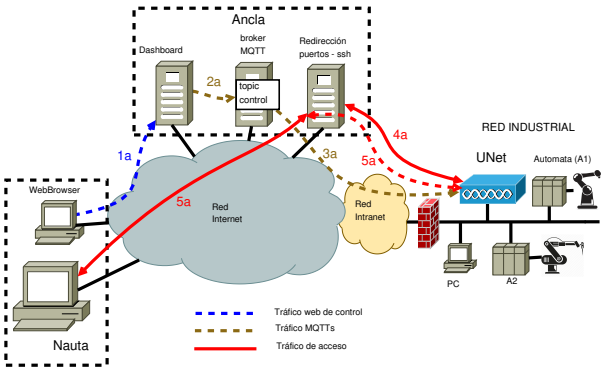


Figure 3: Topología de la plataforma de control de acceso. Flujo de control.

- Flujo de monitorización (topic: "monitor"). Figura 4.
  - Publicación del estado de los servicios de acceso desde el *UNet*. Constarán del estado de activado/desactivado del servicio de acceso y los parámetros asociados. En la Figura 4, el UNet publica en el topic "monitor" del broker MQTT el estado de los servicios de acceso remoto (flujo 1b).
  - Suscripción del *dashboard* al topic "monitor" y recepción del estado de los servicios (flujo 2b).
  - El *Nauta* visualiza el estado de los servicios de acceso en la interfaz web del *dashboard* (flujo 3b) .

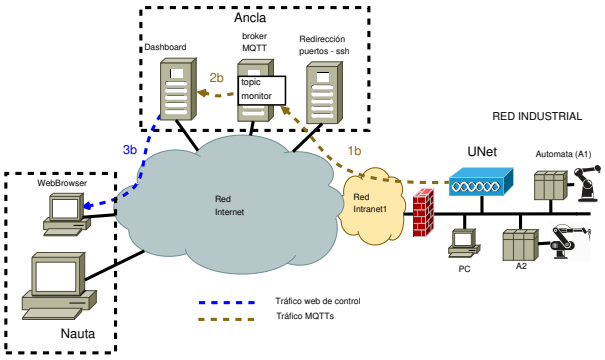


Figure 4: Topología de la plataforma de control de acceso. Flujo de monitorización.

Por simplicidad en el diseño, en este trabajo el *Ancla* incluye tanto el *servicio de redirección de puertos* como el *broker MQTT* y el *dashboard*, aunque podrían distribuirse en dispositivos separados sin afectar a sus principios de funcionamiento.

### 3.3.2. *Formato de datos*

El sistema MQTT es flexible en el etiquetado y organización de los datos, incluyendo el sistema de topics. Este trabajo sugiere una organización de los mismos en la Figura 5. En la Sección 4 se plantea una opción híbrida basada en topics y payloads parseados en formato *json* para la diferenciación de los diferentes servicios, acciones y parámetros.

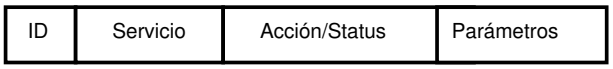


Figure 5: Formato del payload de datos MQTT

Como servicios de acceso se proponen *SSH* y *VPN* (Tabla 1), pero pueden incluirse TerminalServer, RemoteDesktop, VNC o cualquier otro. La etiqueta json será "service".

Table 1: Servicios de control de acceso MQTTs. Etiqueta "service".

| código json | descripción |
|---|---|
| *sshd* | acceso al servicio *SSH* |
| *vpnd* | acceso al servicio *VPN* |

Como acciones se proponen arranque, parada y recopilación de información (Tabla 2). Pueden incluirse otras si el *UNet*, el *Ancla* o el *Nauta* lo permiten. La etiqueta json será "action".

Table 2: Acción de control de acceso MQTTs. Etiqueta "action".

| código json | descripción |
|---|---|
| start | arranque del servicio de acceso. |
| stop | parada del servicio de acceso. |
| status | captura de información. |

La Tabla 3 presenta los parámetros, que dependerán de los campos "service" o "action" del payload MQTT.

Table 3: Parámetros de control de acceso MQTTs

| etiqueta json | valor |
|---|---|
| UNetIPPub | IP pública del *UNet* |
| UNetIPPriv | IP privada del *UNet* |
| UNetPortLocal | puerto del servicio de acceso en el *UNet* |
| UNetPortAnchor | puerto de acceso al *UNet* en el *Ancla*. |
| UNetPID | PID del servicio |
| AnchorDNS | Nombre de dominio del *Ancla* |
| AnchorIP | IP pública del *Ancla* |
| AnchorPort | puerto del servicio de redireccion en el *Ancla*. |
| AnchorUser | usuario de acción de redirección en el *Ancla* |

### 3.3.3. *Proceso en el* UNet

El dispositivo *UNet* que habilita el acceso a la red industrial ejecuta un software que permite la escucha de las publicaciones en el topic "control" del broker MQTT y la ejecución de las acciones pertinentes en función de las órdenes recibidas en ese topic. A la finalización de dichas acciones publica el resultado de las mismas en el topic "monitor". La Figura 6 presenta un diagrama de flujo de la ejecución del software en el *UNet*.

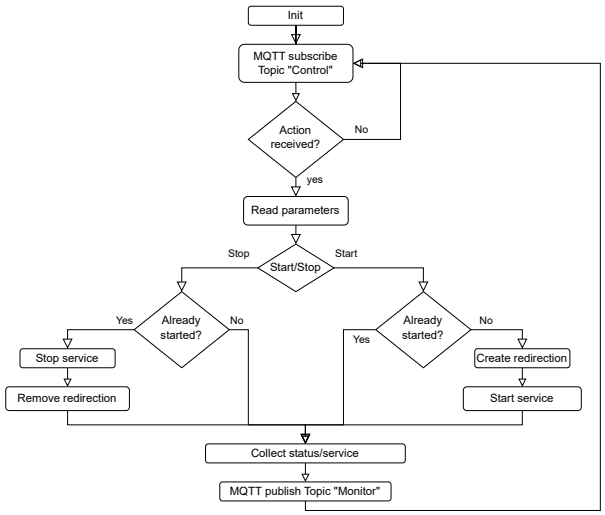


Figure 6: Ejecución del *servicio de control de acceso remoto* en el *UNet*.

## 4. Ejemplo de caso de uso

Se presenta un *servicio de control de acceso remoto* a redes industriales por parte de una empresa que realiza labores de mantenimiento en los PLCs instalados en sus clientes.

En el *Ancla* se implementa el *broker MQTT* ("mosquitto"), el *dashboard* ("NodeRed") y el *servicio de redirección de puertos* (implementado con "OpenSSH"), siendo los tres servicios accesibles desde Internet. La plataforma es Linux. El *Nauta* es un dispositivo de usuario con la suite de Siemens TIA-Portal, un navegador web, un cliente ssh y un cliente *VPN* OpenVPN. El *Nauta* accede tanto al servicio *dashboard* como al *servicio de acceso remoto* a la red industrial.

Cada red industrial tiene un *UNet* consistente en un dispositivo Raspberry Pi 3B+, el lenguaje de programación de scripts Python3, la suite OpenSSH de cliente y servidor *SSH* y un servidor *VPN* OpenVPN. Cada *UNet* dispone de un topic, y sobre él, están los topics "control" y "monitor". Los dispositivos *UNet* se codifican con el nombre UNet-XY donde XY es un número de dos dígitos, y su topic asociado tiene el mismo nombre. El intercambio de los mensajes de control y monitorización encapsulados en MQTT entre el dashboard y cada uno de los UNet se realiza en el topic "UNet-XY/control" y "UNet-XY/monitor". La Figura 7 muestra el caso de uso.

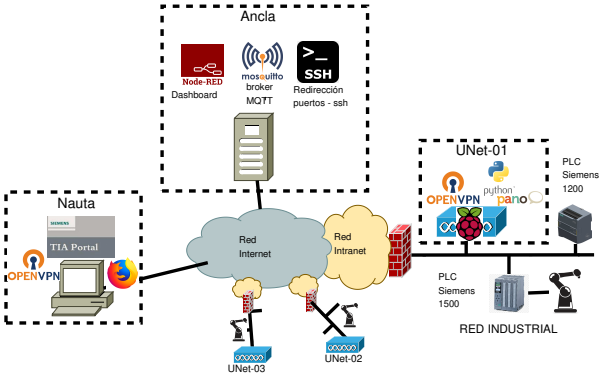


Figure 7: Topología del caso de uso.

El *UNet* utiliza la librería "paho" de Python para la implementación del diagrama de software de la Figura 6. La securización MQTTs se hace mediante TLS.

El pseudocódigo python mostrado en Code 3 presenta las acciones tras la lectura de un mensaje en el topic "control" al que está suscrito el *UNet*, (en el caso del UNet-01 sería al topic "UNet-01/control").

Code 3: UNet. MQTT subscribe. Recepción de mensaje en topic "Control".

```
def on_msg(client, userdata, msg):
  try:
    payload = json.loads(msg.payload.decode("utf-8"))
    service = payload["service"]
    action = payload["action"]
    BrokerSshPort = payload["AnchorPort"]
    ...
    if service == "sshd":
        if action == "start":
            on_ssh()
        if action == "stop":
            off_ssh()
    if service == "vpnd":
        if action == "start":
            on_vpn()
        if action == "stop":
            off_vpn()
  except Exception as e:
    print("Error", str(e))
```

El pseudocódigo python mostrado en Code 4 presenta como ejemplo las acciones para la activación del sercico de acceso *sshd* en el *UNet*. Primeramente crea la redirección en el *Ancla*, y una vez creada activa el servicio *sshd* en el *UNet*. Para la comprobación de funcionamiento realiza una conexión ssh hacia el puerto remoto del *Ancla* que redirige la conexión hacia el propio *UNet* (RemoteServPort), utilizando un usuario y una clave local del *UNet*. En función del éxito de la conexión, publica un código en el topic "monitor" del broker reservado para cada *UNet*.

Code 4: UNet. Activación del servicio *SSH*.

```
def on_ssh():
    return_code = subprocess.call("ssh -f -N -p {↩
        BrokerSshPort} -R 0.0.0.0:{RemoteServPort}:↩
        localhost:{LocalServPort} {BrokerSshUser}@{↩
        BrokerAddress}")
    if return_code == 0:
        try:
           subprocess.call("systemctl start sshd.service")
           time.sleep(1)
           ssh_client.connect(-p {RemoteServPort} {↩
                UNetUser}@{BrokerAddress} password="↩
                UNetUserPasswd"))
           mqtt_client.publish("Monitor","1")
           except Exception as e:
           mqtt_client.publish("Monitor","0")
        finally:
           ssh_client.close()
    else:
        mqtt_client.publish("Monitor","-1")
```

El *dashboard* ha sido desarrollado utilizando NodeRed. El *dashboard* permite la selección del *UNet*, dispone de botones de activación/desactivación y cuadros de presentación de datos de estado y monitorización. Como atractivo visual se ha incluido un mapa con la ubicación del *UNet* seleccionado. La Figura 8 presenta el resultado de un prototipo sencillo de *dashboard*.

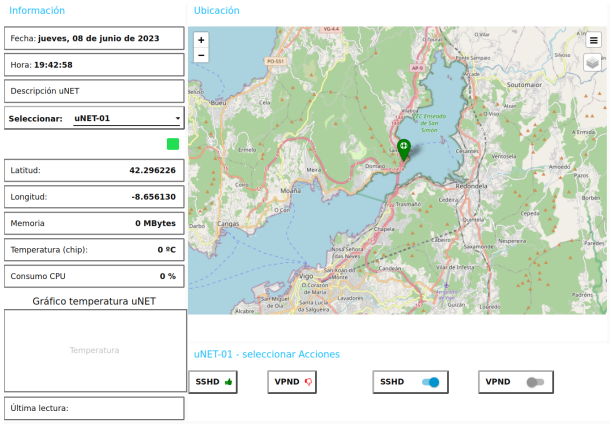


Figure 8: Dashboard desarrollado en NodeRed

Al pulsar "*VPND*" en el *dashboard* desde el *Nauta*, el UNet-01 creará la redirección de puertos en el *Ancla* y arrancará el servicio *vpnd*. En el *dashboard* aparecerá activo o inactivo el servicio *vpnd*. El *Nauta* podrá activar el cliente vpn hacia el *UNet* y podrá acceder con el TIA-Portal a los PLCs instalados en la red industrial para efectuar las labores de mantenimiento remoto sobre los mismos.

## 5. Líneas futuras

Una línea futura clara, habilitará al *UNet* como dispositivo que permitirá no sólo habilitar el acceso *VPN* o *SSH*, sino también recoger datos de monitorización de la red y de los sistemas industriales y enviarlos tanto a servidores en la nube o a servidores locales. Los *UNet* tienen capacidades de procesamiento suficiente incluso para ejecutar acciones directas de control/actuación sobre el sistema de automatización. Para ello será necesario identificar tanto las acciones como los datos a ejecutar o recolectar en el sistema de automatización.

## Agradecimientos

Este trabajo ha sido soportado por el proyecto europeo SM-TMC (586035-EPP-1-2017-1-DZ- EPPKA2-CBHE-JP).

## References

Cisco Cybersecurity Team, 2018. Annual Cybersecurity Report. Tech. rep., Cisco Company.

Diaz-Cacho, M., Gomez, M., Diaz, S., Rodriguez, X., Varela, C., Marcos-Acevedo, J., Chikh, S., 2019. Cybersecurity analysis in soho environments applying the industry iec62443 standard.

Jennings, C. F., Audet, F., Jan. 2007. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP. RFC 4787.
URL: https://www.rfc-editor.org/info/rfc4787
DOI: 10.17487/RFC4787

Lin, D. A. Y., Malis, A. G., Heinanen, D. J., Gleeson, B., Armitage, D. G., Feb. 2000. A Framework for IP Based Virtual Private Networks. RFC 2764.
URL: https://www.rfc-editor.org/info/rfc2764
DOI: 10.17487/RFC2764

OpenVPN Team, 2022. Openvpn. https://www.openvpn.com/, accessed: 2023-06-08.

Secomea Team, 2022. Secomea. https://www.secomea.com/, accessed: 2023-06-08.

Wireguard Team, 2022. Wireguard. https://www.wireguard.com/, accessed: 2023-06-08.

Ylonen, T., Lonvick, C., January 2006. The Secure Shell (SSH) Connection Protocol. RFC 4254 (Proposed Standard).
URL: http://www.ietf.org/rfc/rfc4254.txt