## Siemens IOT2020

Prodotto da Siemens, è un gateway **IoT** progettato e certificato per lavorare in ambienti industriali 24/7 (figura 13). Può essere impiegato per elaborare, analizzare e inviare dati ai più svariati tipi di dispositivi e di reti.

Basato sulla **CPU Intel Quark® x1000** e il sistema operativo open source **Yocto Linux**, dispone di un’interfaccia integrata **mPCIe** che consente di collegare molti dei moduli di espansione disponibili sul mercato (ad esempio per WLAN/Bluetooth).

Un’interfaccia **compatibile con Arduino Uno R3** e con l’**Arduino shield eco system** consente impiegare le stesse shield e di caricarvi la maggior parte degli sketch direttamente dall’IDE di Arduino.

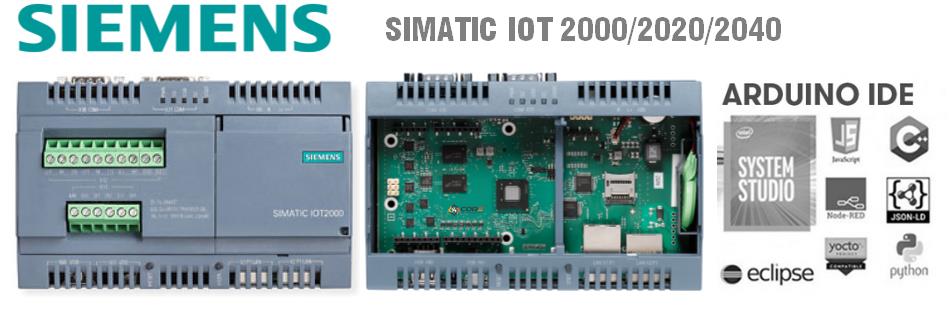


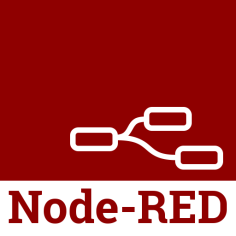
Figura 13

Inoltre, poiché è in grado di utilizzare molti protocolli disponibili e aperti quali Modbus, **Profinet**, REST o MQTT, l’IOT2020 si può interfacciare via Ethernet, o mediante adattatore USB, ad hardware di terze parti come **PLC** e sensori di varie marche.

Può impiegare diversi linguaggi di programmazione ad alto livello come Java, C++ e Python. Inoltre possono anche essere installati **Node-RED**, MQTT e SQLITE3 per connettere e controllare periferiche locali e remote come, ad esempio, i sensori intelligenti.

Di seguito vedremo in dettaglio come abbiamo utilizzato l’ambiente di sviluppo grafico Node-RED sul gateway IOT2020 per realizzare l’interfaccia di supervisione remota del nostro impianto industriale.

## Node-RED

**Node-RED** è uno tra i più noti tool di **flow-based programming** per l’**Internet of Things**. Nasce con l’obiettivo di dare a tutti, anche a chi non è esperto di programmazione, la possibilità di collegare tra loro diversi dispositivi (con eventuali relativi sensori ed attuatori). Inoltre dispone di API e servizi online per poter realizzare sistemi altamente integrati e complessi in modo semplice ed intuitivo.

Dopo aver installato il Sistema Operativo Yocto-Linux sulla SD dell’IOT2020 e dopo averlo collegato alla rete, è possibile installarvi Node-RED attraverso una sessione SSH.

Una volta connessi al dispositivo tramite un client SSH (ex. PuTTY) scriviamo i seguenti comandi:

sudo apt-get update

sudo apt-get upgrade

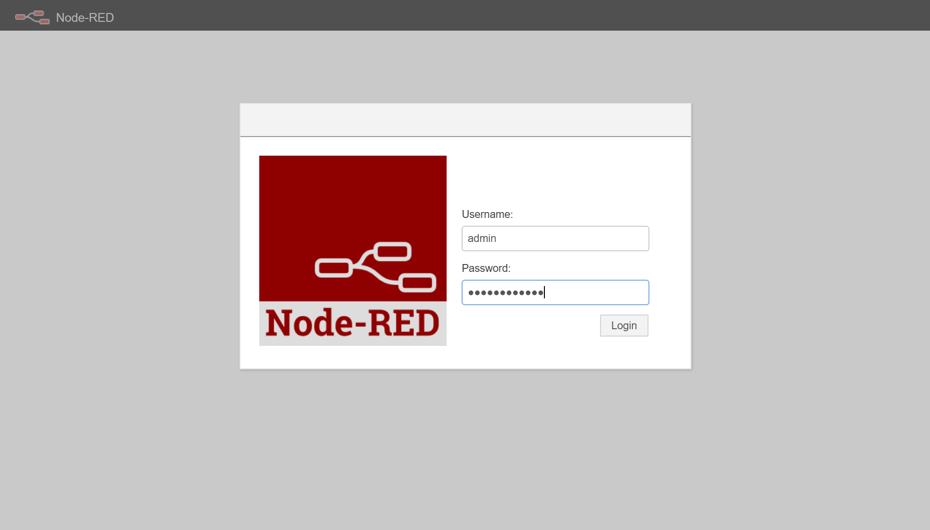
bash <(curl -sL [https://raw.githubusercontent.com/Node-RED/raspbian-deb-package/master/resources/update-nodejs-and-nodered](https://raw.githubusercontent.com/node-red/raspbian-deb-package/master/resources/update-nodejs-and-nodered))

sudo systemctl enable nodered.service

Node-RED-start

A questo punto il servizio è installato e si avvierà automaticamente.

Se adesso, mediante un browser internet, ci colleghiamo all’indirizzo IP di rete dell’IoT2020 alla porta 1880 (http://192.168.0.12:**1880**) apparirà la seguente interfaccia:



Se la restrizione dell’accesso è abilitata, ci verranno richiesti username e password.

Di default tale funzione non è attiva, per abilitarla rimandiamo alla documentazione disponibile al seguente [link](https://nodered.org/docs/security).

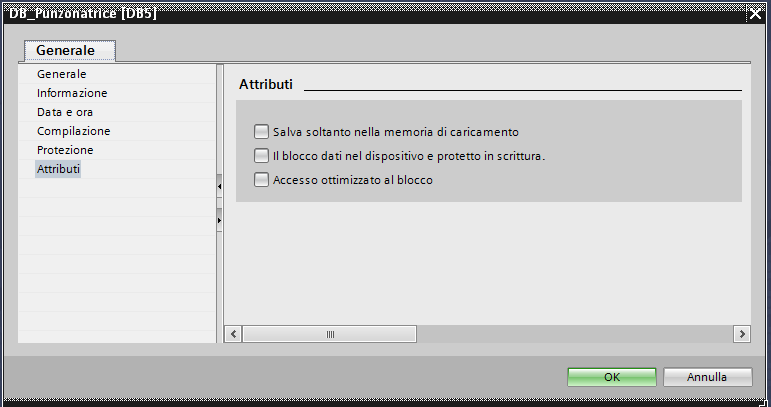
Per poter **comunicare con i PLC Siemens S7-1200** (che utilizzano appunto il protocollo **S7**) è necessario installare un plugin aggiuntivo che ci consentirà la lettura e la scrittura nei **database** (**DB**) dei controllori.

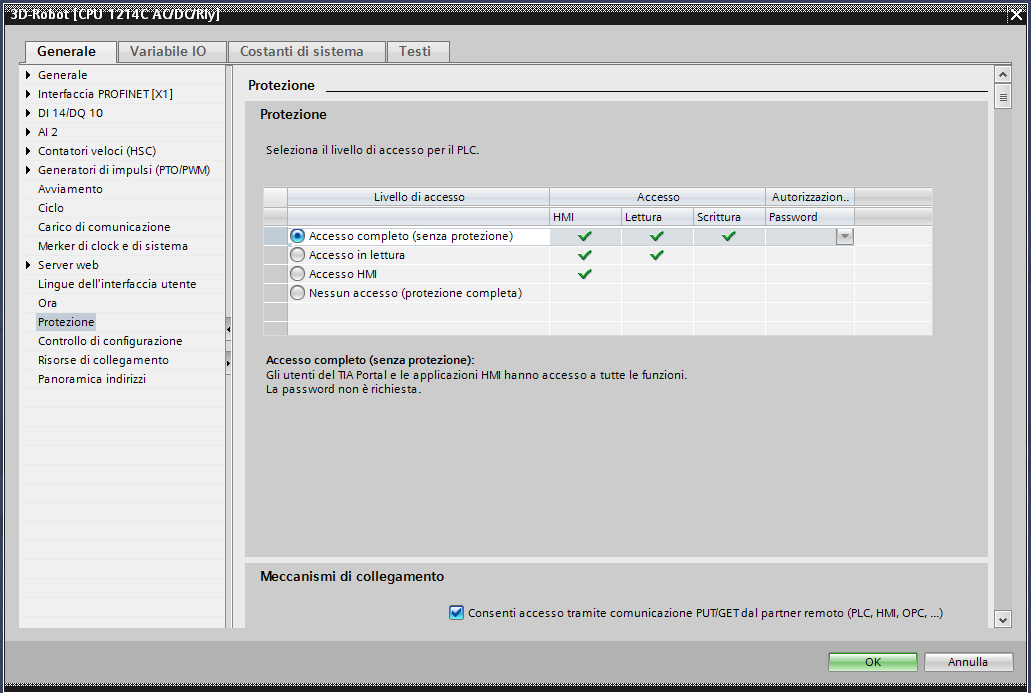
Per aggiungerlo alla suite di Node-RED è necessario andare sul menu “*Manage Palette”* e cercare **Node-RED-contrib-s7**.

Questo plugin usa la versione "base" del protocollo S7, mentre le nuove versioni di firmware dei PLC S7-1200 impiegano una versione "estesa".

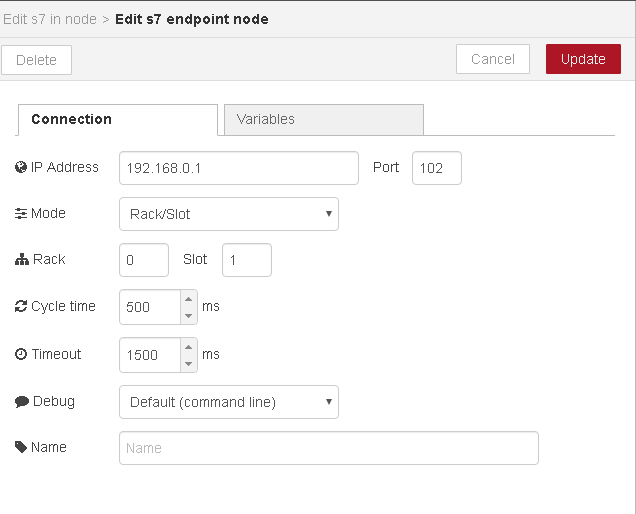
Per poter accedere ai database dei PLC sono pertanto necessari alcuni **passaggi di configurazione aggiuntivi**:

* Nelle proprietà dei DB a cui vogliamo accedere disabilitare la casella di controllo "Accesso al blocco ottimizzato":



* Nella sezione "Protezione" delle proprietà della CPU, abilitare la casella di controllo "Permetti l'accesso con PUT / GET":

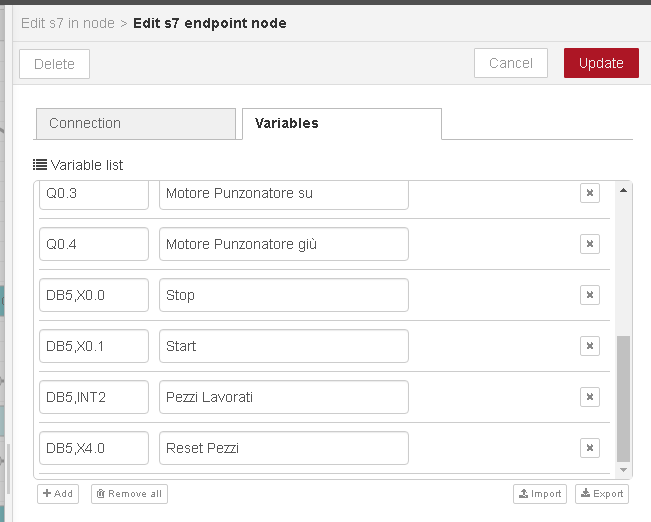
Adesso possiamo aggiungere i nodi che permetteranno lo scambio dei dati con i PLC posti sulla stessa rete a cui è connesso l’IOT2020.

Nella scheda ***Connection*** occorre specificare l’indirizzo IP e la porta (default 102) del PLC con cui vogliamo comunicare.

I valori di *Rack* (*Telaio di montaggio*) e *Slot* (*Posto connettore*) vengono definiti nella configurazione hardware del PLC, visibile in TIA Portal nella scheda *Generale* delle *proprietà* del PLC (default *Rack*=0 e *Slot*=1).

La frequenza di aggiornamento delle variabili viene definita dal valore di *Cycle time*, mentre in caso di errore, trascorso il tempo di *timeout*, sarà effettuato un nuovo tentativo di riconnessione.

L’insieme di queste informazioni identifica un modo univoco un **nodo**.



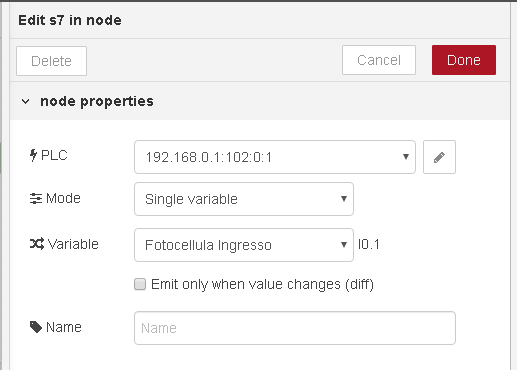
Nella scheda ***Variables*** possiamo inserire la lista delle variabili che vogliamo controllare.

Nella casella di testo a sinistra va inserito l’indirizzo della variabile, mentre in quella di destra il suo nome (può anche essere diverso da quello definito nella tabella delle variabili del PLC).

Come si può notare, in alcuni casi la sintassi utilizzata per accedere ai campi dei database è leggermente diversa da quella usata in TIA Portal. Nella tabella che segue ne sono elencati alcuni esempi:

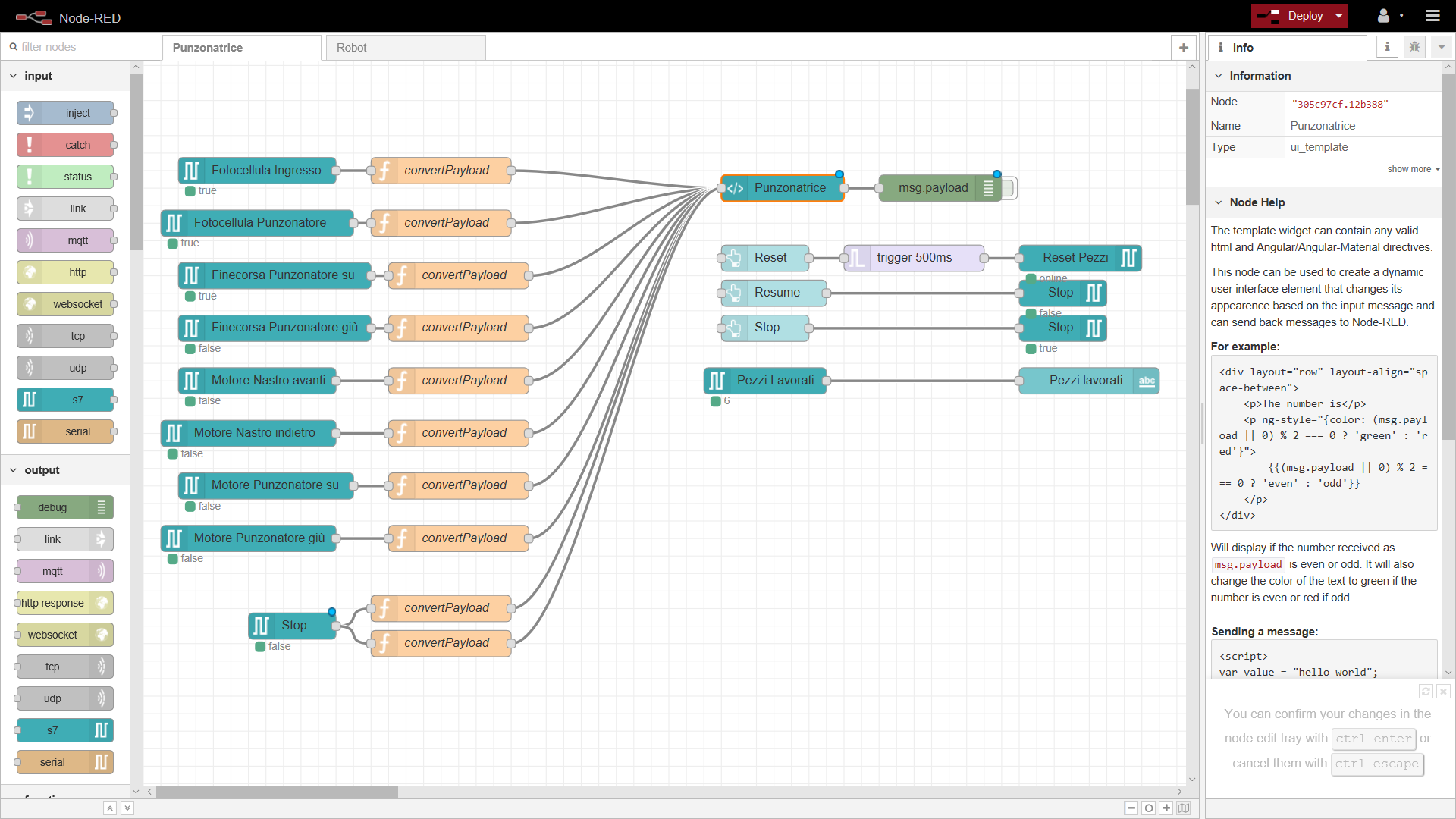
|  |  |  |  |
| --- | --- | --- | --- |
| **Indirizzo** | **Equivalente**  **TIA Portal** | **Tipo di dati** | **Descrizione** |
| DB5,X0.1 | DB5.X0.1 | Bool | bit 1 del byte 0 di DB 5 |
| DB5,B1 o  DB5,BYTE1 | DB5.DBB1 | Byte | Byte 1 (0-255) di DB 5 |
| DB5,I2 o  DB5,INT2 | DB5.DBW2 | Int | signed int a 16-bit dal byte 2 di DB 5 |
| DB57,WORD4 | DB57.DBW4 | UInt | unsigned int a 16-bit dal byte 4 di DB 57 |
| DB13,DI5 o  DB13,DINT5 | DB13.DBD5 | DInt | signed int a 32-bit dal byte 5 di DB 13 |
| DB19,DW6 o  DB19,DWORD6 | DB19.DBD6 | UDint | unsigned int a 32-bit dal byte 6 di DB 19 |
| DB21,DR7 o  DB21,REAL7 | DB19.DBD6 | Real | Floating point a 32-bit dal byte 7 di DB 21 |

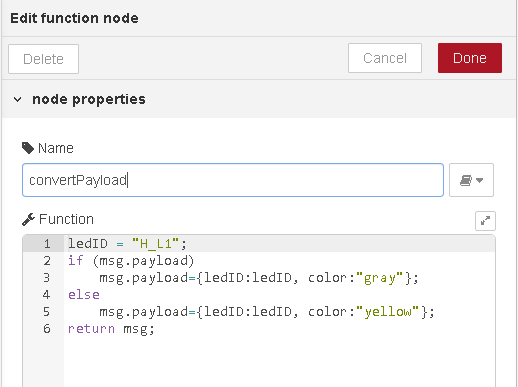
Per leggere i valori delle variabili del PLC è necessario usare il **blocco Input**:

Occorre specificare quale **nodo** si vuole monitorare, la modalità con cui si va a leggere una variabile e il relativo nome.

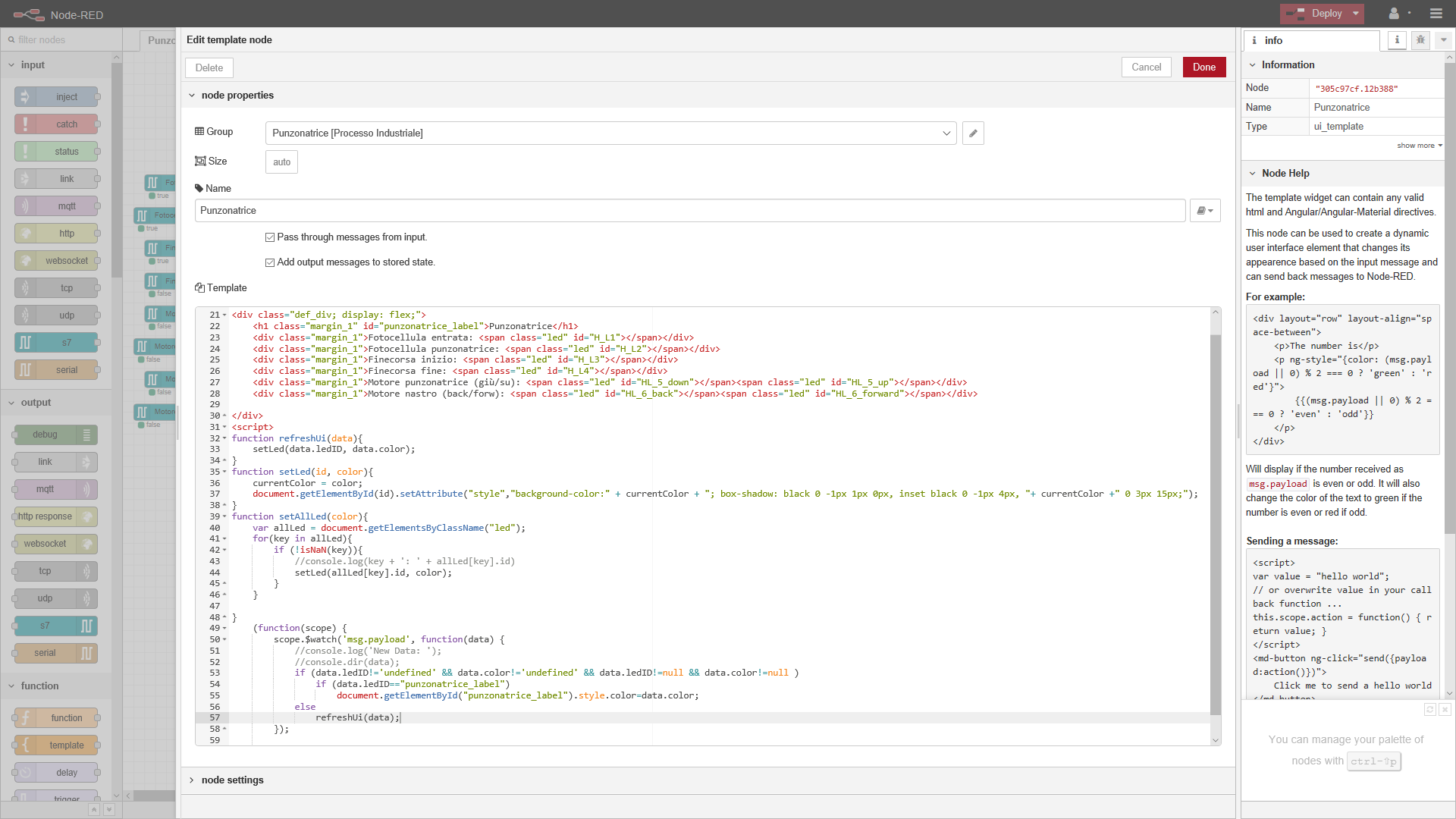
Con l’opzione *“Emit only when value changes (diff)”* è possibile generare un messaggio solo quando c’è un cambiamento di stato e non ogni volta che viene aggiornato l’elenco delle variabili (definito nel *refresh time* del nodo S7).

Per scrivere i valori all’interno delle variabili del PLC è necessario usare il **blocco Output**,configurato in modo simile a quello del blocco input.

Quello rappresentato nella seguente figura è il **flow** completo per la supervisione della macchina punzonatrice. Le variabili vengono lette dal PLC che la controlla per poi essere convertite in un **payload JSON** inviato a una **pagina HTML** contenente tutti i controlli:



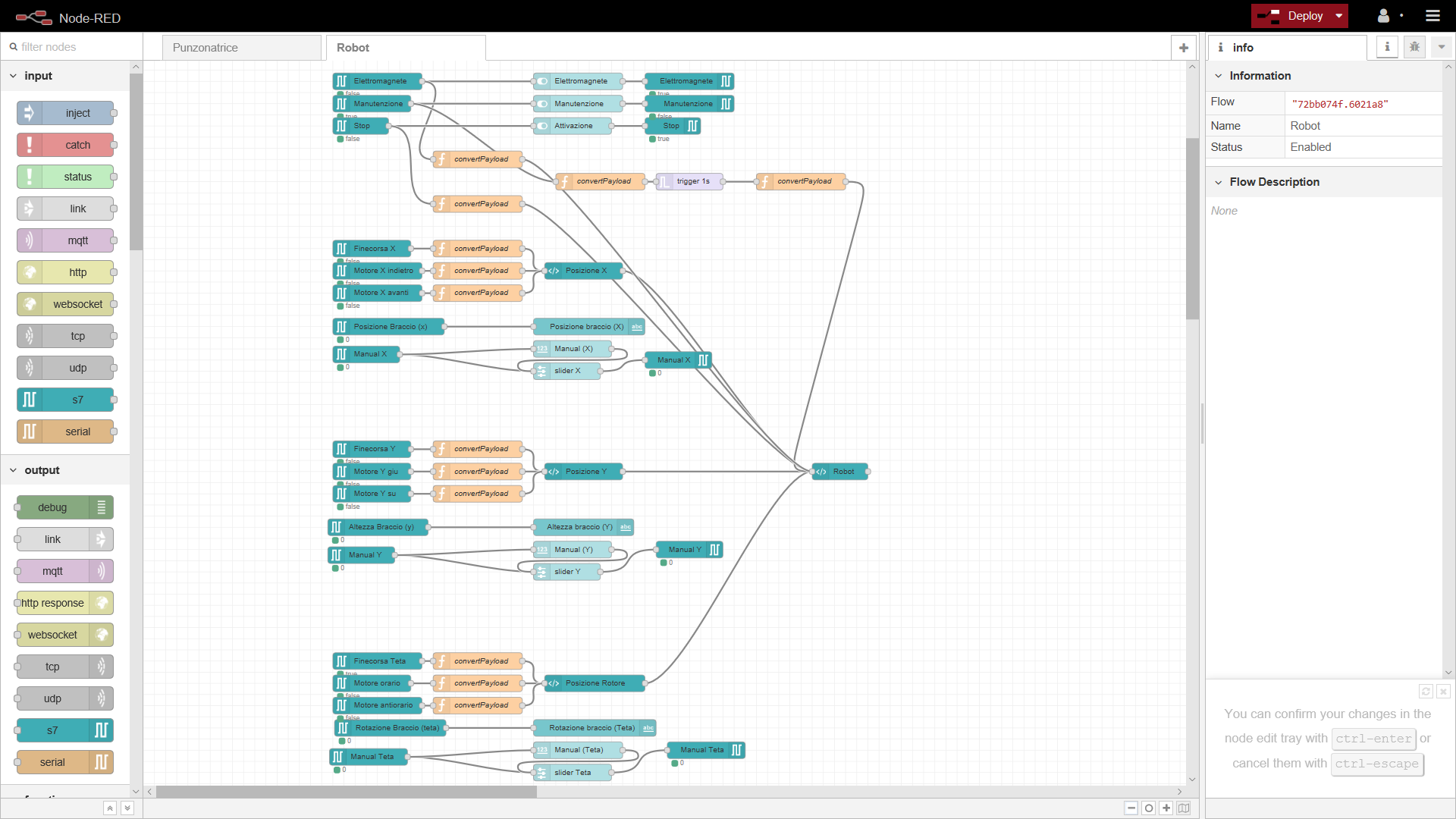
Nella finestra **Edit function node** è possibile convertire una variabile booleana in un payload JSON contenente l’ID associato ad un LED della dashboard e specificare come cambiare il suo colore.



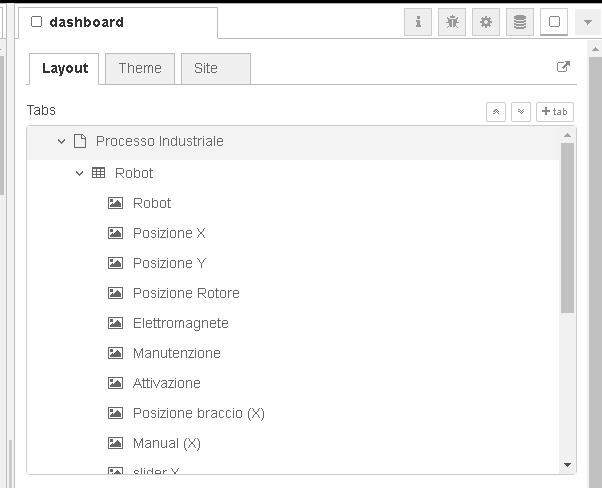
Il **blocco Frame** è composto dai controlli visualizzati nella Dashboard. Il codice è paragonabile a quello di una pagina HTML, con la possibilità di utilizzare **Javascript** (nella figura qui sotto un particolare).

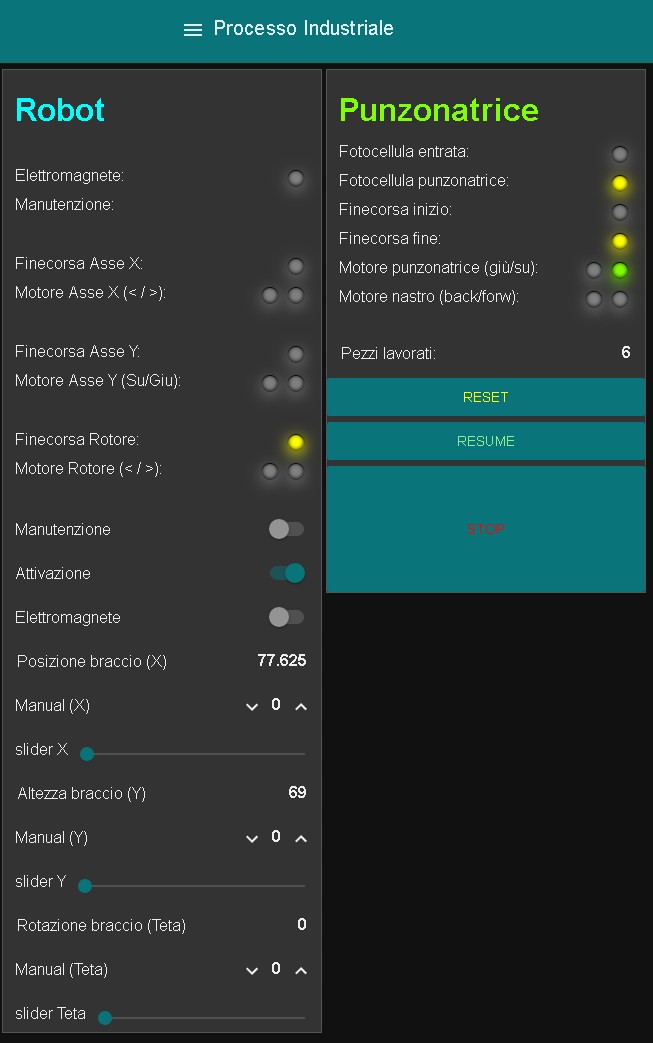


Grazie alle seguenti funzioni è possibile associare ad ogni led un ID, che in questo modo potrà essere controllato attraverso il payload proveniente dalla lettura delle variabili dei PLC.



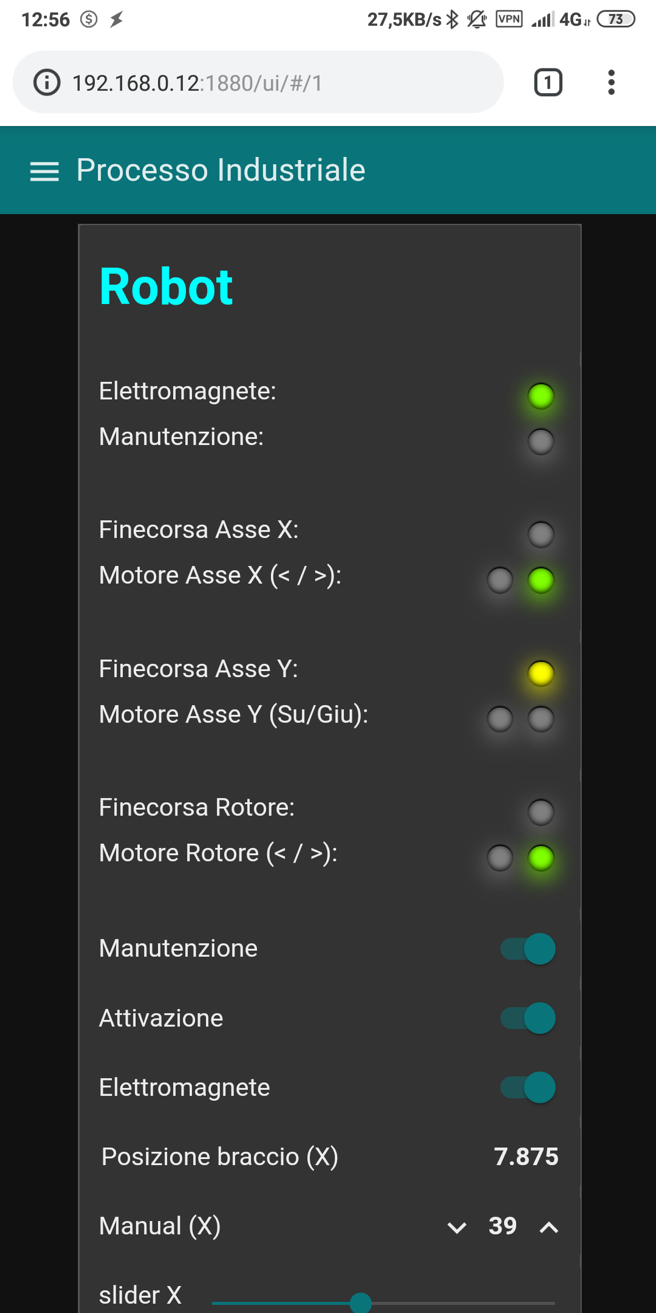
Per il **Robot** abbiamo aggiunto la **possibilità di controllarlo da remoto**, ad esempio, per manutenzione. Pertanto, per modificare le coordinate del suo end effector, abbiamo impiegato dei blocchi “**Slider**” e “**Numeric Control**”.

Tutti gli oggetti vengono successivamente riordinati all’interno della pagina web in base all’ordine assegnato nella sezione **Layout** della dashboard.



Impostando su un browser internet l’indirizzo IP del gateway IOT2020 (nel nostro caso 192.168.0.12) seguito dal numero della porta di default, 1880, viene visualizzata la pagina web generata da Node-RED (**http://192.168.0.12:1880/ui**).

In questo modo è possibile monitorare da remoto lo stato del Robot e della Punzonatrice e, se necessario, intervenire in caso di emergenza o di manutenzione.



Dal momento che vengono utilizzati dei layout dinamici, è possibile visualizzare correttamente la pagina web anche da dispositivi con schermo più piccolo, come palmari e smartphone che, grazie al controllo touch, permettono un controllo più versatile del sistema.

# CYBER SECURITY

Come accennato in precedenza, per motivi di sicurezza, i dispositivi connessi alla rete aziendale non devono avere accesso diretto alla rete di produzione, condivisa dai PLC.

Per accedere alle risorse della rete aziendale, gli utenti devono autenticarsi, solitamente fornendo le proprie credenziali (username e password). Se invece accedono tramite una connessione wireless, devono conoscere anche il nome SSID della rete Wi-Fi e la corrispondente password d’accesso, come richiesto dal **protocollo di sicurezza WPA2**.

Una volta ottenuto l’accesso, **gli utenti autorizzati** avranno la possibilità di raggiungere (attraverso un router/firewall) **solo il** **gateway IOT2020** e, da lì, mediante un browser internet, controllare e supervisionare l’impianto.

Per ulteriore sicurezza abbiamo deciso di non pubblicare su Internet la pagina web creata con Node-RED, ma di renderla accessibile solo dalla rete aziendale.

Gli utenti che hanno la necessità di connettersi da remoto, ovvero dall’esterno della rete aziendale, potranno accedere alla pagina web di supervisione dopo aver effettuato una connessione VPN mobile.

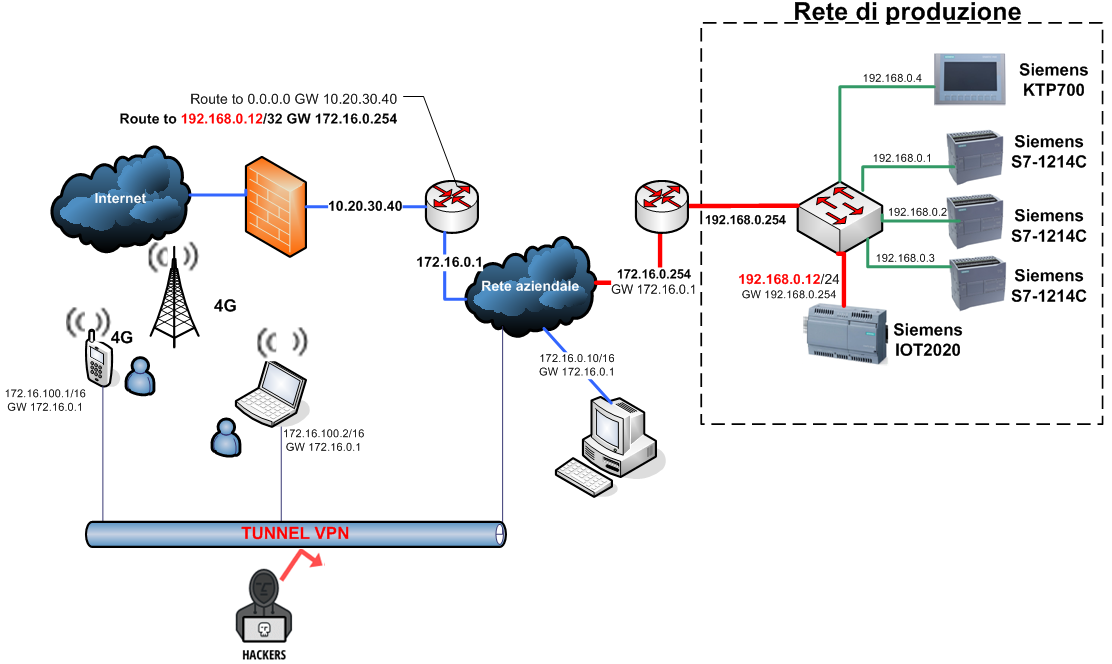
Una **connessione VPN** (**V**irtual **P**rivate **N**etwork) prevede la creazione di un **tunnel virtuale** che, **attraverso Internet**, consente agli utenti remoti di accedere alla rete aziendale con le stesse modalità degli utenti locali.

I dati che transitano attraverso questo canale di comunicazione sono cifrati con protocolli di sicurezza praticamente inviolabili. Inoltre, per accedere alla VPN occorre fornire un’autenticazione aggiuntiva.

In questo modo è sufficiente una connessione dati **4G** o un qualsiasi altro accesso a Internet, per connettere in modo sicuro e da qualsiasi parte del mondo, smartphone, tablet e PC alla rete aziendale.

Premesso ciò, **abbiamo simulato questa situazione** aggiungendo alla nostra piccola rete di produzione un **router** con due interfacce di rete. Una collegata alla LAN dei PLC (192.168.0.0/24), l’altra alla rete didattica (172.16.0.0/16), come mostrato in figura 14.

Abbiamo quindi chiesto al nostro amministratore di rete di aggiungere al router/firewall dell’istituto una regola di routing che instradasse tutti i pacchetti destinati all’IOT2020 (192.168.0.12), e solo a quel dispositivo della rete di produzione, verso l’interfaccia 172.16.0.254 del nostro router (percorso evidenziato in rosso)[[1]](#footnote-1).

In questo modo, attraverso il nostro router, sarà possibile arrivare al gateway IOT2020, anche se è su una rete diversa da quella d’istituto.

I pacchetti eventualmente destinati agli altri dispositivi della rete di produzione, invece, saranno automaticamente scartati dal router dell’istituto perché non esistono altre regole che contengono quelle destinazioni.

Figura 14

Per verificare se da remoto è possibile raggiungere la pagina web di supervisione creata con Node-RED sul gateway IOT2020, abbiamo innanzitutto configurato i nostri smartphone come client VPN.

Ci siamo quindi collegati, mediante la rete dati 4G dei nostri provider, al server VPN dell’istituto (lo stesso router/firewall). Fornite le corrette credenziali di autenticazione, il nostro smartphone ha acquisito automaticamente un indirizzo IP della LAN.

A quel punto digitando sul browser dello smartphone l’URL http://192.168.0.12:1880 siamo riusciti a visualizzare la pagina di accesso di Node-RED anche dal nostro smartphone.

## Conclusione

In questo progetto abbiamo voluto realizzare un esempio applicativo, facilmente riproducibile, dove utilizzando tecnologie tipiche dell’**Industria 4.0**, quali l’**IoT** e la **cyber security**, è possibile, in sicurezza, essere sempre connessi da ogni luogo al proprio impianto di produzione.

1. Diversamente, il router dell’istituto scarterebbe quei pacchetti perché appartengono ad una rete privata che non saprebbe come raggiungere [↑](#footnote-ref-1)