Consorzio PROFIBUS
e PROFINET Italia – P.I.

#PROFIcommunity

Consorzio PROFIBUS
e PROFINET Italia – P.I.

Consorzio PROFIBUS e PROFINET Italia – P.I. #2 - Secondo trimestre 2020

Un ben ritrovati a tutti.

Nuovo appuntamento con il nostro House Organ in un periodo in cui si sta in ogni modo provando a ritornare a una pseudo-normalità, illudendoci forse di poter ritrovare, presto e immutate, le nostre care abitudini pre-pandemia.
Lungi da me nell'addentrarmi in discorsi socio/economico/culturali su come Covid-19 ha cambiato e probabilmente cambierà ancora le nostre vite ma è indubbio che quanto successo, non ancora purtroppo completamente alle spalle, ha avuto influenza anche nella nostra vita consortile.

Raffaele Esposito
Vice Presidente e Tesoriere

Da uomini avvezzi all'automazione industriale poco è cambiato nelle nostre modalità di comunicazione interna ma è chiaramente evidente il fatto che le occasioni per poter illustrare "dal vivo" le tecnologie associate al nostro Consorzio si sono di fatto annullate.

Basti ricordare, ad esempio, come si sia dovuto forzatamente rinunciare alla ormai tradizionale vetrina della Fiera SPS Italia, uno dei momenti di più forte interazione diretta tra Consorzio e potenziali utilizzatori delle nostre tecnologie. Peccato.
Ma non disperiamo: sarà solo uno stimolo per l'anno prossimo a fare ancora meglio di quanto avevamo preparato per questo tribolato 2020.
Non è certo questo, ovviamente, che abbia fatto desistere dal nostro scopo istituzionale, vale a dire la diffusione della conoscenza delle tecnologie PROFINET, PROFIBUS e IO-Link.

Una delle attività in questo senso più concreta che abbiamo deciso di attivare è stata l'organizzazione di webinar gratuiti, attraverso i quali abbiamo pensato di mettere a disposizione dei partecipanti l'esperienza qualificata dei nostri Centri di Competenza.

Tre webinar specifici, su argomenti concreti e subito fruibili, nel più ampio rispetto del nostro classico approccio pragmatico: la manutenzione predittiva su reti PROFIBUS e PROFINET, performance e security per le reti PROFINET e le novità più importanti della tecnologia IO-Link.
Offerta snella, affidata ai nostri esperti, con materiale a disposizione per successivo download dal nostro sito internet: il modo per noi più corretto per "fare cultura tecnica".
Ma non ci fermiamo né ci fermeremo certo qui.
Rimanere aggiornati su tutte le nostre iniziative è estremamente semplice: rimanete sintonizzati sui nostri canali comunicativi.

Insieme all'augurio di una buona lettura non mi resta che augurarvi un sincero buon futuro. Con le tecnologie PROFIBUS, PROFINET e IO-Link lo sarà di sicuro.

Welcome back to all of you.

A new House Organ issue is published, at a time when every one of us is firmly trying to come back to regular life, with a strong hope for returning to the habits we used to have before the pandemic. Far be it from me to talk about Covid-19's influence on socio-economic/cultural aspects and how it has changed our lives, but there is no doubt that what happened – not yet completely ended – has impacted our life at Consorzio PI Italia.

It is true that for industrial automation people like us, internal communications changed only a little. However, it is crystal clear that opportunities to show in person the technologies have been cancelled. For instance, we regrettably had to renounce to our annual meeting at Fiera SPS Italia – a place which offers the strongest direct interaction between the Consorzio PI and the potential users of our technologies.
That's truly a pity. However, do not despair; it serves as motivation for next year to do even better than what we had prepared for the current – turbulent – year. What happened surely did not divert us from our main goal, that is, PROFIBUS, PROFINET and IO-Link technologies' distribution. One of the most definite actions we started was the planning of a free webinar series, to provide the participants with the experience of our RPAs. We offered three specific webinars about practical topics: the predictive maintenance on PROFIBUS and PROFINET networks, performance and security for PROFINET networks and the most important IO-Link technology updates. To spread the "technical culture", our experts provided free downloadable materials on Consorzio PI's website at the end of the webinars. But we won't stop here. Stay tuned to our communication channels – website and social media.

With the wish for good reading, all I want to do is wishing you a genuine good future. With PROFIBUS, PROFINET and IO-Link technologies, it certainly will be.

Diagnostica delle reti PROFIBUS e PROFINET

di Micaela Caserza Magro Centro di competenza GFCC

Le reti di comunicazioni possono essere diagnosticate e le informazioni che rendono disponibili sono utili per capire lo stato di salute o di degrado della rete stessa.

Le reti di comunicazione rappresentano lo scheletro di tutto l'impianto definito dalla Industria 4.0, per questo il loro monitoraggio e diagnostica diventa un punto estremamente importante. La sfida è poter integrare direttamente gli allarmi ed i warnings generati dai sistemi di comunicazione in modo da poter avvertire in modo efficace e tempestivo il personale.

La diagnostica delle reti di comunicazione necessità di avere a disposizione strumenti hardware e software per poter analizzare il traffico e dedurre le informazioni necessarie.

Considerando le tecnologie di comunicazione real-time PROFIBUS e PROFINET gli indicatori da considerare sono diversi dato le che tecnologie sono diverse. Il PROFIBUS è un protocollo di comunicazione seriale, in questo caso il punto più critico risulta il livello fisico. Lo strumento da utilizzare è un oscilloscopio ed un analizzatore di protocollo. I dati da considerare sono: il deterioramento della forma d'onda, il presentarsi di messaggi corrotti o di retry.

Per poter procedere alla valutazione delle prestazioni del PROFIBUS è necessario considerare di inserire in parallelo alla rete un sistema per poter copiare il segnale elettrico e quindi procedere ad analizzarlo.

Le funzionalità più importanti di un analizzatore di protocollo PROFIBUS sono:

Oscilloscopio, che permette di valutare la forma d'onda. Da qui è possibile capire se c'è un deterioramento del mezzo fisico, delle interfacce di comunicazione, dei connettori

Analisi dei telegrammi, che permette di identificare l'insorgenza di telegrammi errati o di telegrammi che presentano diagnostica dei dispositivi di campo

Funzionalità di master di classe 2, che è un sistema previsto dal protocollo PROFIBUS per consentire la comunicazione aciclica con i dispositivi in campo. Con questa funzionalità è possibile identificare la diagnostica estesa, verificare la configurazione e la parametrizzazione dei dispositivi di rete

Con i metodi di diagnostica elencati è possibile riuscire a definire delle logiche che permettano di monitorare lo stato di salute complessivo della rete e identificare i margini di sicurezza che rimangono per l'esercizio della rete.

Il PROFINET, invece, è un protocollo real time basato su Ethernet per questo motivo le modalità e gli indicatori sono diversi. In questo caso i problemi legati al mezzo fisico sono sicuramente minori, mentre hanno importanza le problematiche legate al traffico di rete. Per questo è necessario monitorare il traffico di rete, la tipologia di protocolli che possono passare sulla rete, oltre ai tempi di aggiornamento dei singoli io-device e del tempo di ciclo complessivo della comunicazione.

Anche nel caso di reti Ethernet based si pone il problema di avere un punto di presa, cioè un punto in cui sia possibile duplicare il segnale elettrico sul cavo ed analizzarlo con un analizzatore di protocollo. Nel caso di ethernet i metodi per trovare un punto di presa sono due:

- Configurare una porta di uno switch managed con porta di mirror
- Utilizzare un tap.

Configurare una porta di mirror significa entrare nel web server di gestione dello switch e configurare affinché l'intero traffico di una porta sia copiata su una porta di monitoraggio a cui sarà collegato il pc su cui sarà installato il software di analisi del traffico.

Questa soluzione è molto rapida ed efficace, ma può presentare un punto negativo che è rappresentato dal carico sul buffer dello switch. Infatti, il traffico deve essere memorizzato prima di essere reindirizzato, per questo è possibile che una parte del traffico sia non copiato se il traffico sullo switch è troppo elevato.

La soluzione del tap, invece, prevede di installare un nuovo dispositivo in rete che risulta essere trasparente sulla rete, pertanto è privo di MAC address e di indirizzo IP. Il tap permette di copiare, elettricamente, il traffico di una porta su più porte in uscita. Da una delle porte sarà collegato il secondo il dispositivo, mentre sull'altra sarà collegato il pc con l'analizzatore. Il vantaggio di questa soluzione è rappresentato dalla semplicità di installazione e di funzionamento. Lo svantaggio è rappresentato dal fatto che il tap è un carico elettrico per la rete ethernet.

Le variabili e gli indicatori da prendere in esame sono diversi da quelli considerati per il PROFIBUS. In particolare, è importante andare ad esaminare le seguenti variabili:

- Inserimento di nuovi partecipanti nella rete, in questo caso potrebbe essere che sia stato inserito nella rete un nuovo dispositivo che non appartiene alla rete PROFINET, ma che potrebbe invece generare traffico diverso
- Tempi di ciclo della comunicazione, all'aumentare del tempo di ciclo della comunicazione potrebbe esserci un aumento del tipo di traffico non real- time o un problema su alcune delle interfacce di comunicazione dei dispositivi
- Tempi di aggiornamento del singolo dispositivo della rete
- Tipologie di traffico presente sulla rete. Il traffico deve essere prevalentemente di tipo real time PROFINET e con poco traffico di tipo TCP/IP
- Presenza di messaggi scartati, corrotti o elevata presenza di messaggi broadcast o multicast.

Tutti questi indicatori possono mutuamente influenzarsi, ma ognuno di loro è un segnale importante che sulla rete sta succedendo qualcosa di anomalo e le prestazioni non potrebbero rispettare le richieste di progetto.

La possibilità di conoscere gli indicatori del corretto funzionamento delle reti di comunicazioni consente di avvisare in modo efficace e tempestivo gli operatori per

intervenire in modo sicuro sulle cause e mantenere, così, una rete di comunicazione efficiente.
Quello che diventa importante, poi, è poter monitorare in modo continuativo le reti e poter generare allarmi verso gli operatori. La diagnostica ed il monitoraggio delle reti permettono di verificare e identificare l'insorgere di malfunzionamenti o deterioramenti della rete, potendo quindi spostarsi verso quella che può essere definita come la diagnostica preventiva delle reti di comunicazioni. Per fare questo, però, oltre agli indicatori è necessario anche progettare in modo adeguato il sistema di monitoraggio per poter ottenere informazioni importanti. Le tecnologie sono mature per poter ottenere diagnostica, monitoraggio e manutenzione preventiva ma è necessario che queste vengano sfruttate e progettate in modo adeguato.

PROFIBUS and PROFINET networks diagnostics

Communication networks can be diagnosed and the information they make available is useful for understanding the health or degradation of the network itself.
Communication networks represent the entire plant defined by Industry 4.0's framework, so their monitoring and diagnostics becomes extremely relevant. The challenge is to directly integrate the alarms and warnings generated by communication systems so that you can effectively and timely warn your staff.
Diagnostics of communication networks need to have hardware and software tools at their disposal in order to analyze traffic and infer the necessary information.
Considering the real-time communication technologies PROFIBUS and PROFINET the indicators to consider are different given the different technologies.
PROFIBUS is a serial communication protocol, in this case the most critical point is the physical level. The tool to use is an oscilloscope and a protocol analyzer. The data to consider are the deterioration of the waveform, the appearance of corrupt messages or retry.
In order to evaluate the performance of the PROFIBUS, it is necessary to consider inserting a system in parallel to the network in order to copy the electrical signal and then proceed to analyze it.
The most important features of a PROFIBUS protocol analyzer are:

- *Oscilloscope, which allows you to evaluate the waveform. From here it is possible to understand if there is a deterioration of the physical medium, of communication interfaces, of connectors*
- *Telegram analysis, which allows you to identify the onset of incorrect telegrams or telegrams that present diagnostics of field devices*
- *Class 2 master functionality, which is a system provided by the PROFIBUS protocol to allow acyclic communication with devices in the field. With this feature, you can identify extended diagnostics, verify the configuration and parameterization of network devices*

With the diagnostic methods listed, you can define logics that monitor the overall health of your network and identify the remaining safety margins for network exercise.
PROFINET, on the other hand, is a real-time protocol based on Ethernet for this reason the modes and indicators are different. In this case, the problems related to the physical medium are certainly minor, while the problems related to network traffic are important. For this you need to monitor network traffic, the type of protocols that can pass on the network, in addition to the update times of the individual io-devices and the overall cycle time of the communication. Even in the case of Ethernet based networks there is the problem of having a point of socket, that is, a point where it is possible to duplicate the electrical signal on the cable and analyze it with a protocol analyzer.
In the case of ethernet there are two methods for finding a grip point:

- *Configure a port of a managed switch with mirror port*
- *Use a tap.*

Configuring a mirror port means entering the switch management web server and configuring for all traffic on a port to be copied to a monitoring port to which the pc on which the traffic analysis software will be installed will be connected.
This solution is very fast and effective, but it can have a negative point that is represented by the load on the switch buffer. In fact, traffic must be stored before being redirected, so it is possible that some of the traffic is not copied if the traffic on the switch is too high. The tap solution, on the other hand, involves installing a new device on the network that turns out to be transparent on the network, so it lacks MAC address and IP address. The tap allows you to copy, electrically, the traffic of a door on multiple outgoing doors. From one of the ports the second device will be connected, while on the other will be connected the PC with the analyzer. The advantage of this solution is the simplicity of installation and operation. The disadvantage is that the tap is an electrical load for the ethernet network.
The variables and indicators to be examined are different from those considered for the PROFIBUS. In particular, it is important to examine the following variables:

- *Introducing new participants into the network, in this case it may be that a new device has been inserted into the network that does not belong to the PROFINET network, but may instead generate different traffic*
- *Communication cycle times, as the communication cycle time increases there may be an increase in the type of non-real-time traffic or a problem on some of the device communication interfaces*
- *Update times of the individual network device*
- *Types of traffic on the network. Traffic must be predominantly real-time PROFINET and with little TCP/IP traffic*
- *Presence of discarded, corrupted or high presence of broadcast or multicast messages.*

All of these indicators can mutually influence each other, but each of them is an important signal that something abnormal is happening on the network and performance may not comply with project requests.
The ability to know the indicators of the proper functioning of communications networks allows you to effectively and timely alert operators to take safe action on the causes and thus maintain an efficient communication network.
What becomes important, then, is being able to continuously monitor networks and be able to generate alarms towards operators. Network diagnostics and monitoring allows you to verify and identify the occurrence of network malfunctions or deteriorations, thus being able to move towards what can be defined as the preventive diagnostic of communications networks. To do this, however, in addition to the indicators it is also necessary to properly design the monitoring system in order to obtain important information. Technologies are mature to achieve diagnostics, monitoring and preventative maintenance, but they need to be properly exploited and designed.

Conciliare performance e security nelle reti industriali PROFINET

di Paolo Ferrari Centro di competenza CSMT

Con l'avvento della rivoluzione digitale sono cambiate anche le reti di comunicazione usate nelle macchine a livello di campo. Per attivare i percorsi di raccolta dati specifici dei processi Industry 4.0, bisogna interfacciare le machine ad internet, creando dei collegamenti che fino a qualche anno fa erano inesistenti.

La necessità d'interconnettere le macchine crea una esigenza diffusa di security, ossia di protezione della parte di produzione delle nostre aziende nei confronti di accessi indesiderati, non solo di natura malevola ma anche accidentali. Se in precedenza la security era ignorata dai costruttori di macchine (che si limitavano, per esempio, a proteggere con password il proprio PLC), oggi la security è obbligatoria per tutti, a tutti i livelli.

Purtroppo, concetti di sicurezza per gli ambienti office non possono essere "semplicemente" trasferiti alle reti di automazione. Le misure di sicurezza implementate per i sistemi di automazione non devono essere in conflitto con i requisiti operativi relativi ai protocolli real-time.

Per ottenere il massimo livello di sicurezza ragionevole per i sistemi e le reti di automazione, è essenziale un processo di gestione della sicurezza che includa una analisi dei rischi (di solito i rischi di impianti produttivi differiscono dai rischi normalmente considerati nel mondo IT), delle misure organizzative / tecniche coordinate e una ripetizione periodica o su evento.

Un approccio che può soddisfare i vincoli posti dai sistemi di produzione è quello definito "difesa in profondità", ossi la stratificazione di diversi meccanismi di difesa che rendono complicato e costoso realizzare accessi indesiderati. Con questo metodo tra l'altro è possibile dotare di protezione anche sistemi che non sono stati nativamente pensati per essere sicuri (esempio, i sistemi di comunicazione usati in industria da ormai decine di anni).

Fa parte di questo processo di protezione in profondità il concetto di segmentazione della rete. Ampiamente applicato nel settore IT, consiste nel suddividere tramite firewall la rete in tante sottoreti e poi regolare gli accessi tra le varie zone.

Questo efficace approccio però deve essere approfondito nel caso delle reti real-time (come ad esempio PROFINET) perché in ambito industriale al livello produzione ci sono molti altri fattori che devono essere considerati per la suddivisione. Stiamo infatti considerando sistemi fisici reali, sottoposti a vincoli incoli meccanici, vincoli normativi, necessità di interfacce uomo macchina, norme sulle postazioni di lavoro e relativa ergonomia.

PROFINET permette di rispettare queste esigenze di security garantendo delle performance applicative sempre ottimali.

Naturalmente ci sono alcune semplici regole che vanno rispettate nella progettazione:

- Usare strutture basate su una backbone realizzata interconnettendo switch managed, da cui si diramano i rami secondari. Questo permette di avere a disposizione una dorsale capace non solo di supportare un elevato traffico, ma anche di filtrare e bloccare eventuale traffico indesiderato immediatamente.
- Assegnare a tutti gli switch managed password sicure diverse da quelle di default
- Creare un solo punto di accesso alla rete di macchina permette di proteggerne meglio l'accesso.
- Razionalizzare e gestire gli accessi VPN, estraendo il traffico dal tunnel criptato prima di arrivare a livello di rete di automazione, in modo da filtrarlo secondo le regole del firewall di macchina.
- Evitare le porte di rete liberamente accessibili a bordo macchina che venivano tradizionalmente installate per facilitare la vita ai manutentori ma che oggi diventano punti di accesso non controllato.
- Evitare l'introduzione indiscriminata di access point wireless (anche in modo temporaneo) che possono facilmente diventare punti di accesso non controllato alla rete
- Tenere periodicamente monitorato l'elenco dei partecipanti alla rete di automazione e i livelli di traffico in modo da evidenziare immediatamente eventuali problemi legati ad accessi non autorizzati.
- Tenere in conto che molti protocolli IT generano traffico nella rete, se indiscriminatamente installati nelle reti di

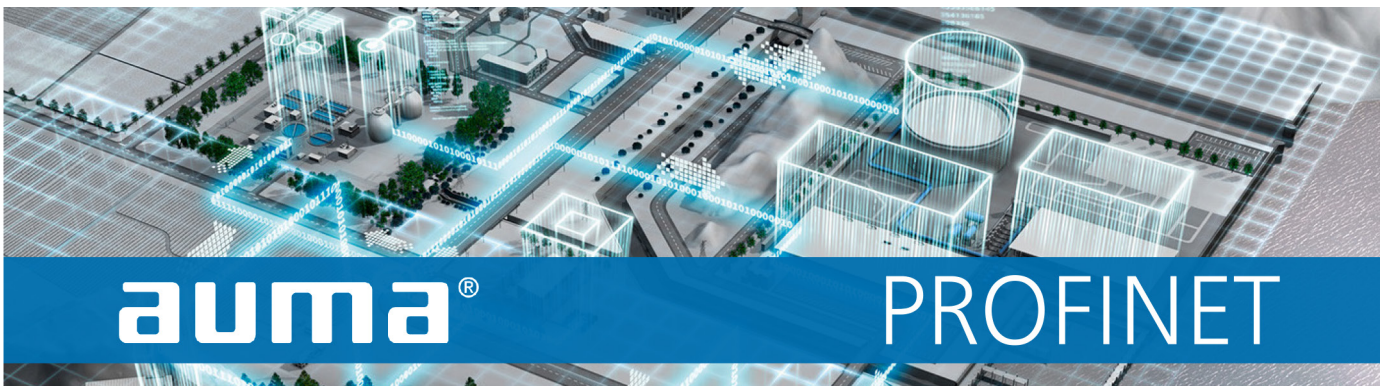
automazione potrebbero creare situazioni di conflitto con le operazioni di tipo real-time dell'automazione.
Infine, è da sottolineare che PROFINET sta attivamente lavorando per modificare la situazione e per introdurre ulteriori livelli di sicurezza a livello di applicazione real-time. Per esempio, è previsto l'uso di una autenticazione per poter partecipare alla funzione di controllo e l'aggiunta di una funzione di controllo dell'integrità per impedire l'uso di dati alterati.
In conclusione, nelle reti PROFINET è possibile far convivere security e performance rispettando semplici regole di progetto e adottando chiare politiche di security armonizzate con la parte IT dell'azienda.

Reconciling performance and security in PROFINET industrial networks

At the beginning of the digital revolution, the communication networks employed in the field-level machine have also changed. To start data collection paths for Industry 4.0 processes, you need to interface machines to the internet, to create links that until a few years ago were completely non-existent.
The need to interconnect machines creates a widespread need for security, to protect against unwanted access, not only malicious ones but also accidental ones. If security was ignored by machine builders (who were limited, for example, to password-protecting their PLC) in the past, today security is mandatory for everyone, at all levels. Unfortunately, security concepts for office environments cannot be "just" transferred to automation networks. The security measures, which are implemented for automation systems should not conflict with operational requirements for real-time protocols. To achieve the highest reasonable level of security for automation systems and networks, a security management process – which includes a risk analysis – is essential (usually the risks of production facilities differ from the ones of the IT section), coordinated organizational/technical measures, and periodic or event repeat.
One approach that can meet the constraints of production systems is called "in-depth defence". This means layering different defence mechanisms which make it complicated and expensive to make unwanted access.
With this method, among other things, it is also possible to equip systems that have not been designed to be safe (i.e. the communication systems used in industry for decades).
The "in-depth defence" also includes network segmentation. Widely applied in the IT sector, it consists of dividing the network into many subnets through firewalls and then adjusting the accesses between the various zones. However, this approach needs to be investigated when applied to real-time networks (such as PROFINET) because many other factors need to be considered in the industrial sector at the production level.
We are considering actual physical systems, which are bound to mechanical and regulatory constraints, to human-machine interfaces and workplace rules and related ergonomics.
PROFINET allows meeting such security needs, ensuring optimal application performance. Of course, there are a few simple rules that must be respected:

- *Use structures based on a backbone, which is built by interconnecting managed switches, from which the secondary branches start. This allows the user to have a backbone, which is capable not only of supporting high traffic but also of filtering and blocking any unwanted traffic immediately.*
- *Assign all managed switches secure passwords – other than the default ones.*
- *Creating a single access point to the machine network helps to better protect its access.*
- *Rationalize and manage VPN access, extracting traffic from the encrypted tunnel before arriving at the automation network level, so that it is filtered according to the rules of the machine firewall.*
- *Avoid the freely accessible network ports onboard the machine that were traditionally installed to make life easier for maintainers but which today become uncontrolled access points.*
- *Avoid the indiscriminate introduction of wireless access points (even temporarily) that can easily become uncontrolled access points to the network*
- *Keep regular monitoring of the list of participants in the automation network and traffic levels to immediately highlight any issues related to unauthorized access.*
- *Keep in mind that many IT protocols generate traffic on the network, if they are indiscriminately installed on automation networks, they could create conflict with real-time automation operations.*

Finally, it should be noted that PROFINET is actively working to change the situation and introduce additional layers of security at the real-time application level. For example, you would use authentication to participate in the audit function and add an integrity check function to prevent the use of altered data.
In conclusion, in PROFINET networks it is possible to coexist security and performance by respecting simple project rules and adopting clear security policies harmonized with the IT part of the company.



IO-Link e la quarta rivoluzione industriale

di Serena Fortunati Centro di competenza DUPLOMATIC

Nato nel 2006 all'interno di un workgroup tecnico del Consorzio PROFIBUS e PROFINET International, IO-Link, in quasi 15 anni di vita, ha fatto tanta strada. Ogni anno è cresciuto al passo con le richieste di mercato. Oggi, anche grazie all'avvento della quarta rivoluzione industriale, caratterizzata dalla digitalizzazione, è diventata una presenza costante nel settore industriale. Perché?! Vediamo insieme qui di seguito.

In questi ultimi anni, il mercato globale, compreso quello industriale, è stato caratterizzato da tre parole predominanti: digitalizzazione, sicurezza e semplificazione.

Da una analisi più puntuale, quella rivolta all'innovazione e alla tecnologia, possiamo anche osservare come queste tre parole sono spesso legate tra di loro. Quando leggiamo un argomento sulle nuove tecnologie digitali, spesso troviamo riferimenti alla loro sicurezza, sia essa fisica o "digitale", e alla loro semplicità di utilizzo o integrazione.

IO-Link ne è un esempio concreto: è il protocollo di comunicazione che digitalizza l'ultimo metro della connessione ad una macchina e in un processo industriale; per questo, trasmette un dato meno disturbato - quindi più sicuro al controllo centrale -, integrandosi nel sistema esistente in modo semplice.

Questo esempio ci fa intuire il motivo per cui IO-Link, in questi ultimi 5 anni, ha triplicato la sua diffusione nel mercato, passando da circa 5 milioni di nodi a 16 milioni.

La sempre più diffusa presenza di questo protocollo di comunicazione è, inoltre, ben visibile da altri fattori, quali: l'aumento del numero di costruttori di dispositivi IO-Link, ad oggi circa 322; il crescente numero di Community IO-Link con diffusione globale, di cui l'ultima nata in Giappone; e la formazione di Centri di Competenza in diversi paesi che, grazie al loro know-how tecnico in materia, supportano i costruttori di dispositivi e macchine nell'integrazione di IO-Link. Di questi, gli ultimi nati sono: uno in Italia in Duplomatic MS e uno negli Stati Uniti in Pepperl + Fuchs Comtrol, Inc.

Parliamo ora delle novità di IO-Link e facciamolo utilizzando le tre parole protagoniste di questi ultimi anni evolutivi.

Iniziamo dalla prima parola: digitalizzazione.

Quando parliamo di digitalizzazione in IO-Link, ci riferiamo a quest'ultima in connessione al mondo della Industria 4.0.

A partire dal 2016, infatti la Community IO-Link ha iniziato ad integrare le specifiche di base con diverse novità per il trasferimento dei dati di diagnostica dalla rete industriale alla rete IT e al Cloud. Ha iniziato con l'introduzione di IO-Link Wireless, limitato però alla comunicazione tra Master IO-Link Wireless e Device IO-Link Wireless, per poi passare all'integrazione più recente, con i protocolli MQTT e OPC UA. Questi ultimi sono entrambi protocolli M2M standard realizzati per la connessione al mondo del web. Sono molto diffusi, anche se solo il secondo specificamente nel settore industriale.

La possibilità di IO-Link di interfacciarsi direttamente con questi protocolli di comunicazione rende l'acquisizione e la raccolta dei dati di diagnostica totalmente indipendente dal sistema di controllo e da costruttori specifici. Il Master IO-Link, infatti, può, contemporaneamente, essere sia un Gateway IO-Link/Bus di Campo sia un Gateway IO-Link/OPC UA e/o IO-Link/MQTT.

Questa indipendenza rende maggiormente fruibile l'accesso ai dati del campo raccolti da IO-Link, anche da reti sicure ed esterne al processo.

Il risultato è evidente: analisi di diagnostica, utilizzabile anche per la manutenzione predittiva, sempre aggiornata e disponibile in database e programmi già totalmente dedicati allo scopo.

A completamento di questa rete parallela per il collegamento dell'ecosistema IO-Link all' IoT, di recente è stato anche avviato il progetto per gestire il dato di diagnostica acquisito dalla rete IO-Link in formato JSON. Si tratta di uno standard utilizzato per lo sviluppo di pagine web e ha la caratteristica di poter trasferire dati strutturati in modo semplice, leggero ed efficiente; quindi in completo accordo con la filosofia IO-Link.

Passiamo ora alla seconda parola: sicurezza che, in ambito industriale, si traduce in Functional Safety.

La comunicazione in accordo con gli standard di sicurezza funzionale, nell'ambito industriale, è ormai diffusa da più di 20 anni con diverse funzioni e dispositivi specifici presenti trasversalmente su tutta la piramide della rete.

Come per gli altri protocolli di comunicazione industriale, anche IO-Link, a completamento della rete Safety fino al campo, ha redatto le specifiche Safety come estensione delle specifiche di base.

L'approccio di IO-Link Safety sull'integrazione nella rete rimane il medesimo di quello di una comunicazione IO-link normale. Il Master IO-Link Safety, infatti, raccoglie in un unico nodo, e quindi in un'unica interfaccia lato controllo, diversi segnali e dispositivi - siano essi con comunicazione digitale semplice Safety (OSSDe), con comunicazione IO-Link Safety o con comunicazione digitale semplice no Safety (SIO).

Completando una rete bus di campo già Safety anche con IO-Link Safety diventa possibile estendere la funzione di sicurezza sull'intera macchina, dotando questa di numerosi altri FS-Devices raccolti in pochi nodi e facilmente integrabili nel sistema esistente.

Per quanto riguarda la configurazione e i test del dispositivo IO-Link Safety, come per gli altri dispositivi IO-Link, è possibile continuare a gestirli anche off-line, con l'utilizzo di tool e file IODD specificamente dedicati.

A livello di roadmap, ad oggi sono state già pubblicate le specifiche per la realizzazione dei dispositivi dotati di

protocollo IO-Link Safety, di cui sono in pubblicazione le specifiche di test per la certificazione.
Il mercato è, quindi, ormai prossimo a poter utilizzare anche questi dispositivi per garantire la sicurezza completa sulle macchine prodotte.
Ed ecco la terza e ultima parola che caratterizza, non solo IO-Link per la sua essenza, ma anche la sua evoluzione: la semplificazione.
I diversi protocolli di comunicazione industriale includono i cosiddetti "profili", attraverso cui viene specificata l'organizzazione dei dati da comunicare in funzione della tipologia di dispositivo (ad esempio sensore, attuatore o altro). I profili non sono dipendenti dal costruttore, ma dal protocollo di comunicazione che si utilizza e dalla tipologia di dispositivo che comunica, standardizzando quindi il formato dei dati scambiati.
Ciò consente una forte semplificazione perché la presenza di un profilo permette la sostituzione di un dispositivo con un dispositivo equivalente, ma di un altro costruttore, o con un modello più recente, senza richiedere la riprogettazione del sistema di automazione; questa, infatti, continuerà a "vedere" gli stessi dati organizzati nello stesso modo. Le uniche condizioni sono che venga mantenuto lo stesso protocollo di comunicazione e che entrambi i dispositivi utilizzino lo stesso profilo.
IO-Link, protocollo che già uniforma - e quindi semplifica - cablaggio, connessione e comunicazione a livello del campo, ha anche predisposto la comunicazione su profili.
Nella sua roadmap le prime specifiche pubblicate sono state: il Common Profile, che più che un profilo rappresenta una linea guida di specifiche base comuni a tutti i profili IO-Link, e lo Smart Sensor Profile, ovvero il profilo dedicato ai sensori, dispositivi per i quali è nato il protocollo.
Tra i profili IO-Link merita una menzione particolare quello nato per poter aggiornare il Firmware dei prodotti elettronici più complessi sfruttando direttamente la comunicazione IO-Link: il BLOB Transfer & Firmware Update, le cui specifiche sono state recentemente aggiornate (2019).

Oggi, in un mercato in forte crescita ed espansione, anche la necessità di avere ulteriori profili dedicati a dispositivi diversi "no sensor", cresce all'interno della Community IO-Link. È per questa ragione che recentemente sono iniziati due nuovi progetti dedicati alle famiglie degli attuatori e delle lampade, identificati rispettivamente come IO-Link smart actuator profile e IO-Link_Lighting.
IO-Link, è, dunque, un protocollo relativamente giovane e "al passo con i tempi", capace di accogliere ed evolvere le sue specifiche insieme al mercato.
Ma come abbiamo potuto leggere in questo articolo, tutte le novità ed evoluzioni di IO-Link portano in grembo il suo seme originale, ovvero l'idea di creare una rete di comunicazione digitale in campo, universale, facilmente integrabile e scalabile, e, soprattutto, a disposizione di tutti.

IO-Link and the fourth industrial revolution

Born in 2006 as part of PROFIBUS and PROFINET International's technical working group, IO-Link has come a long way in its 15 years of life. Every year it has grown accordingly to market demands. Today, thanks to a fourth industrial revolution, which is characterized by digitalization, it has become a constant presence in the industrial sector. Why?! Let's take a look down below.

In recent years, the global market, including the industrial market, has been characterized by three leading topics: digitization, security and simplification.
From a more precise analysis, which is addressed to innovation and technology, we can see how these three words are often linked to each other. When we read about new digital technologies, we often find references to security, both physical or "digital", and their simplicity in use and integration.
IO-Link is a concrete example of this: it is the communication protocol which digitizes the last meter of the connection to a machine in an industrial process. For this reason, it transmits a less disturbed data - therefore safer to the central control - integrating into the existing system in a simple way.
This example gives us an insight into the reason why IO-Link has tripled its reach in the market in the last 5 years, from about 5 million knots to 16 million.
The increasingly widespread presence of such communication protocol is also noticeable thanks to other factors, such as an increase of IO-Link device manufacturers (currently about 322);

Il **Consorzio PROFIBUS e PROFINET Italia – P.I.** raggruppa in Italia oltre 70 aziende che condividono le tecnologie **PROFIBUS**, **PROFINET** e **IO-LINK** e che combinano la loro esperienza e professionalità per trasformare le idee in standard, gli standard in prodotti innovativi e i prodotti innovativi in soluzioni complete per l'automazione.

the growing number of IO-Link communities with global reach, the latest has been established in Japan; and the training of RPAs in several countries which, thanks to their technical know-how, support device and machine manufacturers in the integration of IO-Link. The latest RPAs: Duplomatic MS (Italy) and Pepperl - Fuchs Comtrol, Inc. (United States).

I'd like to talk about IO-Link's updates through the three leading terms of the last evolutionary years.

Let's start with the first one: digitization.

When we talk about digitization in IO-Link, we mean the connection with it to the world of Industry 4.0.

From 2016, the IO-Link Community began to include the basic requirements with different innovations for diagnostic data transfer from the industrial network to the IT network and to the Cloud. It began with the introduction of IO-Link Wireless, firstly with limited communication between Master IO-Link Wireless and Device IO-Link Wireless, then including the latest integration with the MQTT and OPC UA protocols. The latter are both standard M2M protocols for web connection. They are extremely widespread, although only the second one is specifically employed in the industrial sector.

The capability of IO-Link of directly interfacing with these communication protocols makes diagnostic data acquisition and collection completely independent from the control system and specific manufacturers. Indeed, the Master IO-Link can, at the same time, be both an IO-Link/Field Gateway and an IO-Link/OPC UA Gateway and/or IO-Link/MQTT.

This autonomy makes access to field data collected by IO-Link more manageable, even from secure and external networks.

The result is pretty evident: always updated diagnostic analysis, which can also be used for predictive maintenance, and available in databases and programs.

In order to complete this parallel network for connecting the IO-Link ecosystem to the IoT, a project to manage the diagnostic data acquired by the IO-Link network in JSON format has recently started. It is a standard used for web pages development and its feature allows to transfer structured data in a simple, light and efficient way – in full agreement with the IO-Link philosophy.

Let's now move on to the second term: safety which, in the industrial field, means Functional Safety.

Communication in accordance with functional safety standards in the industrial sector has been widespread for more than 20 years with different functions and specific devices present across the entire network pyramid.

As for other industrial communication protocols, IO-Link, in addition to the Safety network to the field, has finalized the safety requirements as an extension of the basic ones.

IO-Link Safety's approach to network integration remains the same as the normal IO-link communication. The Master IO-Link Safety collects in a single node (therefore in a single control side interface) different signals and devices – both digital communication Safety (OSSDe), with IO-Link Safety communication and simple digital communication no Safety (SIO). It is possible to extend the safety function on the entire machine with IO-Link Safety equipping it with other FS-Devices collected in a few nodes and easily integrated into the existing system.

The configuration and testing of the IO-Link Safety device, as with other IO-Link devices manage can still be managed offline thanks to specifically dedicated IODD tools and files.

At the roadmap level, devices with the IO-Link Safety protocol's implementation requirements have already been published.

The market is now close to using such devices to ensure complete safety on the machines.

Here it comes the third and last term which distinguishes, not only IO-Link but also its evolution: simplification.

Different industrial communication protocols include so-called "profiles", through which the data organization communication is specified according to the type of device (e.g. sensor, actuator or other).

The profiles are not dependent on the manufacturer, but on the communication protocol used and the type of device; thus, the format of exchanged data is standardized. This allows more simplification as the presence of a profile allows a device replacement with an equivalent one. However, the latter is made by another manufacturer or is a newer model, without remodeling the automation system; indeed, it will continue to "see" the same data organized in the same way. It will work only if the same communication protocol is maintained and if both devices use the same profile.

IO-Link, a protocol that already uniformizes - and therefore simplifies - wiring, connection and communication at the field level, has also prepared communication on profiles.

Its first published features were: the Common Profile, which sets a guideline of basic specifications for all IO-Link profiles, and the Smart Sensor Profile, that is, the profile dedicated to sensors – the very reason why the protocol was developed.

Among the IO-Link profiles a special mention for the one who is capable of updating the most complex electronic products' firmware by directly exploiting the IO-Link communication: the BLOB Transfer & Firmware Update, whose features have recently been updated (in 2019).

Now, in a growing and expanding market, the need to have additional profiles for different "no sensor" devices is also growing within the IO-Link Community. For this reason, two new projects for actuators and lamps sector have recently started, respectively: IO-Link smart actuator profile and IO-Link_Lighting.

So, IO-Link is a relatively young protocol and "in step with the times", which is capable of evolving its features according to the market.

However, as we could read in this article, all IO-Link updates keep the original seed: the ambition of creating a digital communication network in the field which will be universal, easily integrated and scalable, and available to everyone.

Direttore responsabile
Giorgio Santandrea

Redazione
NSA srl

Sede legale Via Curtatone 16, Milano **Tel.** +39 02 36685328
Email segreteria@profi-bus.it **P. IVA** 11432840152