



Lirrompere sulla scena della comunicazione industriale di protocolli Ethernet-based anche per applicazioni di controllo di processo e manifatturiero ha fatto sì che si prospettino all'orizzonte nuove applicazioni in termini di reti, in particolare si rendono possibili le cosiddette reti 'ibride'. Con rete ibrida si intende una rete industriale multiprotocollo che condivide un'infrastruttura comune. Il grande vantaggio offerto dalle reti ibride è quello di avere un'unica infrastruttura di rete sulla quale appoggiare l'intero traffico, pur mantenendo le prestazioni attese da ciascun protocollo. Questo ovviamente è possibile unicamente usando come mezzo fisico Ethernet, che garantisce una larghezza di banda sufficiente per la coesistenza multiprotocollo e che assicura le prestazioni. Per verificare queste ultime, nel laboratorio Mailab dell'Università di Genova è stata costruita una rete ibrida di prova che supporta i seguenti protocolli con esigenze di realtime: IEC 61850 (standard per la comunicazione delle sottostazioni elettriche) e Profinet I/O (standard per l'automazione industriale); a questi due protocolli è stato aggiunto del traffico non realtime di tipo TCP/IP proveniente da videocamere per la sicurezza. Una rete di questo genere rappresenta la soluzione più semplice ed economica per integrare tutti i mondi che possono essere presenti in un'azienda: controllo di processo, supervisione della distribuzione elettrica e sistemi di sicurezza.

COESISTENZA... FRA LE RETI

LE RETI DI COMUNICAZIONE IBRIDE SI PRESENTANO
COME LA 'NUOVA GENERAZIONE' DELLA
COMUNICAZIONE INDUSTRIALE

di Micaela Caserza Magro*, Paolo Pinceti *

Part#	Title
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	Principles and Models
7.2	Abstract Communication Service Interface (ACSI)
7.3	Common Data Classes (CDC)
7.4	Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	Mappings to MMS (ISO/IEC 9506 - Part 1 and Part 2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	Sampled Values over Serial Unidirectional Multidrop Point-to-Point link
9.2	Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

Fig. 1 - Struttura dello standard IEC 61850

Le reti ibride

Una rete ibrida utilizza un'infrastruttura Ethernet condivisa per la trasmissione di protocolli di comunicazione diversi. Lo scopo del lavoro qui presentato è verificare se due o più protocolli Ethernet-based possono coesistere sulla stessa infrastruttura di comunicazione senza

precludere le prestazioni realtime richieste dai protocolli stessi, oltre a garantire il funzionamento dei diversi protocolli senza provocare malfunzionamenti o fermate. L'interesse per le reti ibride è molto forte in quanto il loro impatto è notevole sulle architetture e le installazioni future. Rappresentano infatti la migliore soluzione per l'implementazione delle reti di comunicazione: utilizzo di un'unica infrastruttura, semplificazione del cablaggio e, soprattutto, uniformità della topologia d'infrastruttura sull'intero impianto industriale. Come anticipato, la rete ibrida di test è stata configurata utilizzando i due protocolli industriali realtime IEC 61850 e Profinet I/O, questo permette di integrare sulla stessa rete tutti i componenti tipici di un sistema di automazione: Scada, PLC e/o SoftPLC, switch Ethernet, dispositivi di I/O interfacciati con un protocollo di comunicazione industriale, in questo caso Profinet I/O, dispositivi elettrici intelligenti (IED) interfacciati con un protocollo di

comunicazione industriale dedicato, in questo caso IEC 61850. I vantaggi per gli utilizzatori di una rete ibrida sono costituiti dal disporre di un'architettura di rete molto semplice; un'infrastruttura di rete condivisa, con utilizzo di cavi standard; componenti di rete standard; possibilità d'integrazione di altre applicazioni (ERP, streaming video dalle telecamere di videosorveglianza ecc.). Infine, ogni protocollo funziona in modo nativo e non vi è bisogno di inserire nell'infrastruttura di rete gateway o interfacce di comunicazione che possono ridurre le prestazioni temporali del protocollo.

I protocolli implementati: IEC 61850

Lo standard IEC 61850 è nato con lo scopo di eliminare la grande quantità di cablaggi tradizionali presenti in una sottostazione elettrica. Supporta due tipologie di comunicazione: lo scambio dati realtime necessario per le funzioni d'intervento delle protezioni e controllo; la comunicazione off-line necessaria per la configurazione, parametrizzazione e diagnostica dei dispositivi in campo. IEC 61850 è in realtà una famiglia di dieci standard, ognuno dedicato alla descrizione e standardizzazione di una particolare funzione e alla descrizione dei test di conformità. IEC 61850 definisce anche i livelli 1 e 2, che sono quelli Ethernet sia rame

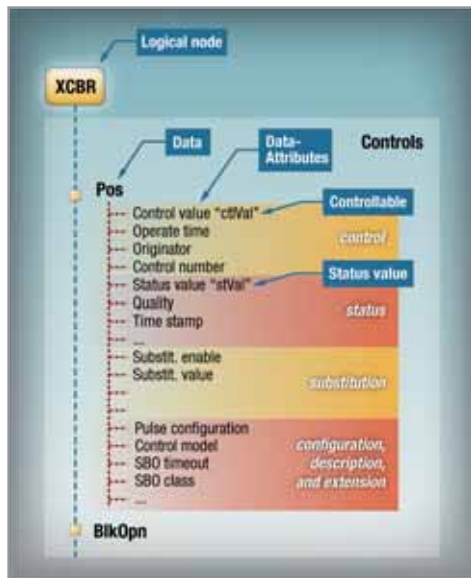


Fig. 2 - Struttura di un nodo logico

sia ottico. Oltre ai primi due livelli fisico e data link lo standard definisce il linguaggio di programmazione che deve essere utilizzato per la configurazione degli IED, chiamato SCL (Substation Configuration Language) basato su XML e che permette di descrivere, in modo standardizzato, tutti gli equipment della sottostazione e delle interconnessioni. A questo si aggiunga che per ottenere un meccanismo affidabile di comunicazione è necessario definire in maniera rigorosa il modello dei dati utilizzati. Proprio per questo motivo il core dello standard consiste nella definizione delle strutture dati, delle metodologie per accedervi e di come queste collezioni possono essere assemblate. Con queste basi diventa anche molto facile garantire l'interoperabilità tra componenti, infatti, definendo a priori le informazioni e i metodi per accedervi, ogni dispositivo può facilmente lavorare con qualsiasi altro nodo della rete. Questa metodologia proviene dal mondo dell'informatica, in cui la definizione delle classi e dei rispettivi attributi e metodi rappresenta la base per la generazione di un programma ben strutturato. Come descritto nella sezione 5 le varie funzionalità della sottostazione vengono suddivise in una serie di nodi logici (Logical Node). Ogni nodo logico si compone delle classi di dati definite nella sezione 7. Le Common Data Class (CDC) contengono una serie di attributi con una semantica prefissata e con una metodologia di scambio predefinita. L'insieme dei nodi logici costituisce il Logical Device, ovvero la rappresentazione logica di un dispositivo reale, per esempio una protezione. Lo standard nella sezione 7 prevede l'utilizzo di quattro classi elementari, con i quali è possibile modellare qualsiasi tipo di dispositivo lo-

gico. Le regole per unire questi blocchi sono derivate direttamente da quelle utilizzate per la composizione delle classi. 'Server' rappresenta il comportamento visibile verso l'esterno di un device. Un server ha il ruolo di gestire la comunicazione con i client device e inviare informazioni, per esempio le misure campionate, agli altri server. 'Logical Device' (LD) contiene le informazioni gestite e condivise tra diverse applicazioni residenti nel device stesso, chiamate Logical Node. 'Logical Node' (LN) contiene le informazioni necessarie all'implementazione della funzione a cui il logical node fa riferimento. 'Data' rappresenta il valore d'interesse con tutti gli attributi che servono a descriverlo. Si può accedere ai dati all'interno di un LN in due modi: attraverso un meccanismo di tipo client-server (Gossops - Generic Object Model for Substation and Feeder Equipment) utilizzando un generico browser Web (comunicazione di tipo non realtime); attraverso un meccanismo di tipo publisher-subscriber (Goose - Generic Object Oriented Sub-

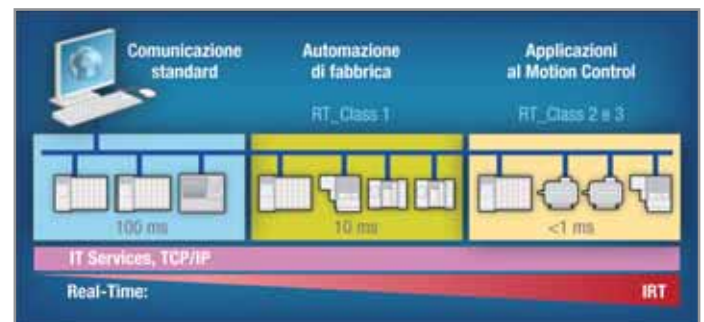


Fig. 3 - Tipologie di comunicazione supportate da PNIO

station Events) per la comunicazione realtime. Questo meccanismo permette di inviare i dati ogni 4 ms in forma di broadcast; i dati che vengono trasmessi sono raggruppati all'interno di un data set.

I protocolli implementati: Profinet I/O

Profinet I/O è un protocollo di comunicazione per il controllo dei dispositivi remoti da campo impiegato nel settore dell'automazione industriale. Ha come peculiarità quello di essere stato progettato per rispondere ai requisiti provenienti dall'automazione dei processi manifatturieri, in cui i vincoli temporali e di realtime sono stringenti. Pertanto, le prestazioni di Profinet I/O devono essere in termini di tempi di risposta e di numero di oggetti con cui scambiare i dati. Proprio per queste peculiarità è uno switched Ethernet, che garantisce le prestazioni migliori in termini di risposta temporale. Sua caratteristica principale è supportare tutti i tipi di comunicazione: non realtime, realtime (RT) e realtime isocrono (IRT), per questo è adatto anche a essere impiegato in applicazioni in cui sono richieste prestazioni di hard realtime. Al momento attuale Profinet I/O trova il suo naturale campo di applicazione nell'ambito del motion control e per creare una backbone ad alta velocità nel mondo del controllo di processo; si prefigge l'obiettivo di trasmettere i dati su un'infrastruttura Ethernet convenzionale (switched), mantenendo però i requisiti prestazionali richiesti dalle applicazioni per cui è nato. I meccanismi che permettono a Profinet I/O di garantire le prestazioni temporali necessarie, oltre a supportare traffico non RT, possono essere così riassunti: assegnazione di priorità ai dati che vengono scambiati, accessi differenziati di sistemi di controllo diversi allo stesso device in campo, descrizione delle funzioni di comunicazione di ciascun device di campo in un file standard GSDml (analogo al file GSD per i device Profibus, ma scritto utilizzando il linguaggio XML) e utilizzo di un meccanismo di scambio dati di tipo provider-consumer.

Le varie classi di comunicazioni gestite in Profinet I/O sono state divise in quattro categorie. La categoria 'Non-RT' viene considerata per la

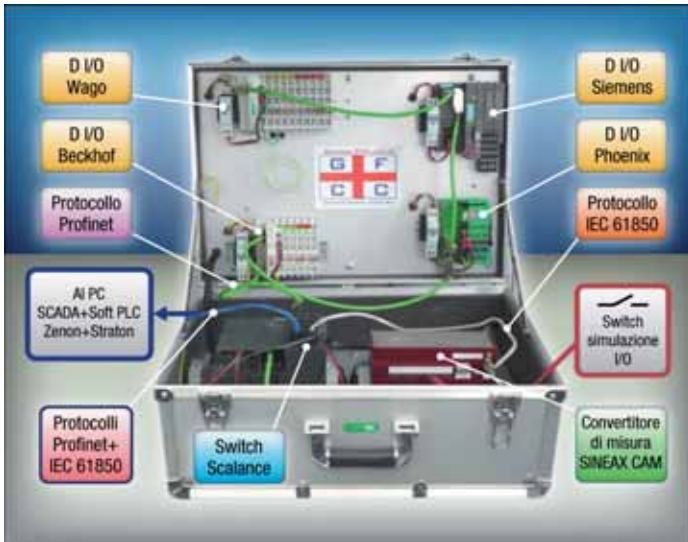


Fig. 4 - La rete di prova

trasmissione di dati di configurazione o per implementare cicli con periodo maggiore ai 100 ms, che tollerino fino al 100% di variabilità. Per la comunicazione si fa affidamento su protocolli standard quali TCP e UDP. Vengono supportati anche servizi ICT, come la gestione della rete Dynamic Host Configuration Protocol (Dhcp), diagnosi di rete Simple Network Management Protocol (Snmp), accesso remoto tramite Web Hyper Text Transfer Protocol (http) e funzioni di posta elettronica. La 'RT Classe 1' può realizzare cicli di pochi ms, tipicamente 1-64 ms, a



Fig. 5 - Rete di test no.1

variabilità contenuta (15%) e si basa sullo standard Ethernet 802.1Q in cui i dati vengono trasmessi tramite telegrammi Ethernet con priorità; per l'implementazione è sufficiente hardware Ethernet standard. Nella 'RT Classe 2', invece, chiamata anche 'IRT-Flex', i frame vengono trasmessi con o senza sincronizzazione, andando a comportarsi come la Classe 1. La sincronizzazione consente tempi di ciclo di 1 ms e tutti i telegrammi possono essere inviati e ricevuti in una finestra temporale definita in fase di progetto e riservata al solo traffico IRT-flex. Il jitter massimo si attesta sui 10 μ s; l'instradamento dei messaggi è fatto in base all'indirizzo MAC e serve hardware Asic per la sincronizzazione. Infine, la categoria 'RT Classe 3', denominata 'IRT-Top' è la più performante, riservata ad applicazioni di motion control. Rispetto alla Classe 2 si ha una più stringente pianificazione temporale del traffico, ottenuta tramite la sincronizzazione tra il livello di rete e l'applicazione software che gestisce i dati. Il ciclo è selezionabile da un minimo di 250 μ s a un massimo di 4 ms con intervalli di 125 μ s. Il jitter è garantito ben

al di sotto del μ s, così facendo si conosce l'istante pressoché esatto d'invio e ricezione di un telegramma IRT-Top. Il determinismo ottenuto prevede precisioni di sincronismo maggiori gestite direttamente dall'hardware. Una stazione (master Sync) ha il compito di inviare il telegramma alle altre stazioni appartenenti al dominio di sincronizzazione. La conoscenza della topologia di rete è fondamentale per la determinazione dei ritardi di trasmissione e, in caso di modifiche sulla topologia o sui rapporti di comunicazione, è necessario riprogettare la configurazione.

La rete di prova

La rete di test messa a punto da MaiLab si compone di una rete Profinet, uno Scada, un SoftPLC e un dispositivo Sineax CAM IEC 61850. La rete Profinet consta di una valigia demo di Gfcc (Genoa Fieldbus Competence Centre) contenente uno switch Siemens Scalance X208, quattro Profinet IO collegati in linea, l'alimentazione e i cablaggi. Il SoftPLC è Straton, un software prodotto da Copa-Data che permette di interfacciarsi a molti dispositivi che parlano diversi protocolli. Il PC sul quale è installato Straton è collegato allo switch Scalance tramite un cavo Ethernet. Straton viene utilizzato come master per configurare i dispositivi della rete Profinet e per ricevere e pilotare le variabili degli stessi. Viene anche impiegato per simulare una protezione Siprotec che si interfaccia tramite IEC 61850. Questo è possibile in quanto Straton implementa il server 61850 e non solo la funzione di client. È stato quindi possibile tramite il file SCL creare il server 61850 che simula il dispositivo e permette di modificare i valori delle variabili.

Lo Scada utilizzato è Zenon, sempre prodotto da Copa-Data, che si collega a Straton e riceve le variabili della protezione visualizzandole su un sinottico a video e consente di effettuare comandi per pilotare la



Fig. 6 - Rete di test no.2

protezione. Zenon si collega anche a un convertitore di misure elettriche Sineax CAM 61850 e, sempre attraverso il sinottico, ne visualizza lo stato. Allo switch Scalance sono quindi collegati: il PC che esegue il runtime di Zenon e Straton, la rete Profinet I/O composta dai quattro dispositivi collegati in linea, il dispositivo Sineax CAM.

La creazione della rete è avvenuta in tre fasi. All'inizio è stata creata la rete 61850 comprendente Zenon e Straton, poi è stata aggiunta la sottorete Profinet I/O, infine sono stati effettuati dei test per controllare se i due mondi riuscissero a comunicare. Utilizzando Straton è stata simulata la protezione partendo dal SCL file e creando un server 61850 che rende disponibili le variabili della protezione stessa al client Zenon, che si collega al server tramite il driver IEC 61850[6] implementato da Copa-Data. Tramite l'editor di Zenon è stato creato il sinottico che mostra a video lo stato della protezione, riportando in tempo reale i valori delle variabili stVal, q e t; inoltre, è stata creata un'interfaccia per comandare la protezione. Lo stesso sinottico viene utilizzato per

monitorare il dispositivo Sineax CAM, riportando in tempo reale i valori delle variabili di stato $stVal$, q e t dei digital input del dispositivo.

Alla rete 61850 è stata collegata la rete Profinet I/O aggiungendo e configurando i dispositivi in Straton. In questo modo, Straton ha sia le variabili della rete 61850, sia quelle dei dispositivi Profinet I/O (I/O digitali). Si è quindi passati a creare una logica tra le variabili delle due reti in modo che potessero comunicare tra loro. La logica implementata ha il fine di integrare i due mondi, così un comando Profinet I/O su un bit di input va a pilotare un interruttore della protezione 61850 che, a sua volta, comanda un bit di output di un dispositivo Profinet I/O. Una volta completata la parte di cablaggio e configurazione della rete si è passati a testare se la rete e la logica implementata permettessero l'integrazione tra i due protocolli e la comunicazione tra i diversi dispositivi.

I risultati ottenuti

Sono state realizzate tre architetture di rete con diversi livelli d'integrazione e in ognuna di esse è stato possibile configurare, comandare e monitorare i dispositivi periferici. Le configurazioni testate variano



Fig. 7 - Rete di test no.3

dalla semplice coesistenza tra i due protocolli sulla stessa rete, alla possibilità di realizzare logiche d'interscambio dei dati provenienti dalle periferie interfacciate con i due diversi protocolli. Rete di test 1: nella prima configurazione viene utilizzato il PLC nativo Siemens Simatic s7-300 della valigia PN1 per generare traffico di rete Profinet. Il PLC configura la rete Profinet I/O assegnando gli indirizzi IP ai dispositivi e configurando gli stessi; il programma che viene eseguito dal PLC forza anche gli output dei dispositivi in modo periodico.

Alla rete Profinet è stato collegato il PC con Zenon e il dispositivo Sineax CAM con le configurazioni precedentemente. In questa configurazione, attraverso lo switch passano sia il protocollo IEC 61850, sia Profinet I/O, ma i due protocolli non condividono lo stesso cavo Ethernet per comunicare. I dispositivi sono nella stessa rete ma non vi è comunicazione tra la parte Profinet I/O e la parte 61850.

Questa configurazione corrisponde a un'architettura che separa la parte di automazione da quella di supervisione, come avviene negli impianti tradizionali. Permette al PLC di eseguire il proprio ciclo, andando a scrivere e leggere sugli I/O periferici, e allo Scada di monitorare il dispositivo Sineax CAM, ricevendo con comunicazione spontanea le variazioni di stato delle variabili acquisite. Rete di test 2: con questa configurazione si è andati a sostituire il PLC Siemens con un master Profinet implementato con SoftPLC ed è stata aggiunta la protezione Siprotec, simulata sempre tramite Straton utilizzando il server IEC 61850. Con questa configurazione si ha il passaggio di entrambi i protocolli sul cavo Ethernet uscente dal PC verso lo switch; il master

Profinet comunica con i quattro dispositivi Profinet, mentre lo Scada comunica con il dispositivo Sineax CAM; la comunicazione tra lo Scada e il server 61850 avviene all'interno del PC. Questa configurazione si differenzia molto dalla precedente, in quanto in questo caso il SoftPLC contiene sia le variabili 61850 della protezione Siprotec, sia le variabili della rete Profinet I/O; ciò permette di realizzare a livello di SoftPLC delle logiche di scambio dati tra le due reti. Si tratta di un'architettura di rete meno comune, in quanto sullo stesso PC si hanno sia la parte supervisione, sia la parte di controllo. È il passaggio intermedio verso la prossima configurazione testata, che prevede la divisione dello Scada e del SoftPLC su due PC. Rete di test 3: questa configurazione differisce dalla precedente in quanto è stata divisa la parte di supervisione, ora installata sul secondo PC, dalla parte di controllo, che risiede sull'altro PC. In questo modo, si torna a un'architettura simile a quella della prima configurazione. Questa configurazione però permette un controllo superiore sulla rete rispetto alla prima, nella quale il PLC era in grado di gestire solo la rete Profinet: in questo caso, utilizzando il SoftPLC che ha a disposizione il driver per IEC 61850, si possono gestire i dispositivi che si interfacciano ai due protocolli facendoli interagire.

Conclusioni

Quanto descritto dimostra come sia possibile integrare tra di loro i due protocolli Profinet I/O e IEC 61850 sulla stessa rete ibrida. È stato anche mostrato come sia possibile ottenere differenti livelli d'integrazione tra i due protocolli. Le possibilità architettoniche offerte dalle reti ibride sono svariate, anche se le tre riportate e studiate sono quelle di maggiore interesse per le applicazioni industriali. Inoltre, le archi-



Fig. 8 - Architettura di rete ibrida

tture di rete ibride si prestano a integrare lo streaming video, supportando la videosorveglianza e le applicazioni di security nella rete di automazione. Ciò risulta molto interessante, poiché permetterebbe di gestire tutto l'impianto di automazione utilizzando un'unica rete ibrida. Come è possibile vedere in figura 8 si utilizza una sola rete ibrida per gestire tutti i componenti di una sottostazione elettrica; si hanno infatti parte elettrica, parte di automazione gestita dal PLC, telecamere di sorveglianza e Scada che comanda e controlla i dispositivi della rete. Questa è solo una delle possibili architetture che si potranno realizzare. Le grandi possibilità che si aprono con la definizione delle reti ibride interesseranno anche il mondo della sicurezza funzionale: la possibilità di far coesistere su una rete ibrida un bus in sicurezza con altri non in sicurezza.

Nota: Gli autori sono del Dipartimento Diten, Università di Genova e fanno parte del Comitato Tecnico Fieldbus & Networks (*)