NUMERO 1 IN ITALIA SU ELETTRONICA EMBEDDED E SEMICONDUTTORI

Firmware 2.0

#29
Dicembre 2022

IoT Cyber Security

IN QUESTO NUMERO:

E MOLTI ALTRI ARTICOLI E PROGETTI!

it.emcelettronica.com

Elettronica Open Source

PROFESSIONAL & MAKER ZONE

Firmware 2.0 EDITORIAL PLAN 2022

COSA LEGGERAI NEL 2022?

TOPICS	MAKERS ZONE	DATA DI PUBBLICAZIONE
IoT	Blockchain/Cryptocurrency	1 Febbraio
AI/ML	Big Data Analytics	1 Marzo
Mems/Sensors	Self Driving	1 Aprile
Wireless/RF	Low Energy Smart Projects	1 Maggio
IoT	Voice Bot/Chat Bot	1 Giugno
Robotics	Cloud Computing	1 Luglio
IIoT/Automation	Smart Monitoring	1 Settembre
LED/Optoelectronics	Wearable	1 Ottobre
Embedded Boards Design	Microcontrollers Projects	1 Novembre
IoT	Cyber Security	1 Dicembre

La sicurezza nei sistemi embedded e IoT

Cari lettori,

è online il nuovo numero della rivista di elettronica Firmware 2.0. All'interno di questo numero potrete leggere articoli tecnici, progetti di elettronica, tutorial e diversi contenuti innovativi sul tema IoT/Cyber Security e sulle tecnologie emergenti. Gli attacchi informatici alle aziende sono cresciuti in modo esponenziale e lo scenario attuale lascia intravedere una possibile escalation futura di questo fenomeno. Per le aziende diventa perciò indispensabile dotarsi di efficaci strumenti di cyber-security per contrastare le minacce, sviluppando strategie di resilienza informatica e prevenzione con l'obiettivo di prepararsi in modo corretto ai potenziali attacchi. Ecco quindi che la cosiddetta cyber-resilienza diventa il nuovo paradigma delle imprese moderne che vogliono soddisfare gli obiettivi di sicurezza richiesti dalla particolare applicazione. Allo stesso tempo, il tema della sicurezza sta diventando un fattore determinante anche nella progettazione dei moderni dispositivi elettronici. Come sappiamo, i sistemi IoT sono in grado di apportare innovazione in molti aspetti aziendali e della vita quotidiana. Pensiamo ad esempio alla capacità dei dispositivi di comunicare con una rete centralizzata per la raccolta dei dati e la ricerca delle informazioni. In seguito alla crescita dei sistemi che includono dispositivi connessi in rete, è aumentata in modo significativo anche la necessità di garantire un elevato grado di sicurezza dei sistemi embedded e IoT. Le minacce a cui sono sottoposte le reti e i dispositivi elettronici interconnessi rappresentano una criticità reale. Proprio in seguito alla diffusione capillare di prodotti elettronici connessi alla rete Internet secondo la filosofia dell'IoT, è diventato necessario porre in primo piano gli aspetti legati alla sicurezza informatica. D'altra parte, tra i fornitori e gli utilizzatori di sistemi embedded e IoT è aumentata la consapevolezza della sicurezza dei dati che scorrono all'interno delle reti, e di quanto sia importante fornire una protezione efficace dei nodi della rete dalle minacce provenienti dall'esterno. I device di ultima generazione, da quelli per la casa intelligente ai dispositivi indossabili, fino alle piattaforme di sviluppo e ai tantissimi sensori digitali per i quali l'evoluzione tecnologica ha portato a un'evoluzione delle metodologie e delle tecniche di attacco da parte degli hacker, richiedono una strategia mirata che coinvolga sia il lato software sia l'hardware, per garantire contemporaneamente la piena disponibilità e affidabilità nel funzionamento e nell'utilizzo dei moderni dispositivi elettronici, nonché la sicurezza degli utenti finali. La complessità del quadro aumenta man mano che prendono forma implementazioni IoT sempre più sofisticate. Pur essendo l'Internet of Things una tecnologia ormai consolidata da anni, negli ultimi tempi il cambio radicale di modalità di lavoro a distanza e l'affermarsi di tecnologie innovative alla portata di tutti hanno spinto notevolmente la sua applicazione nei contesti più disparati. E' quindi facile immaginare quanto le tecnologie alla base dell'IoT stiano raggiungendo un nuovo livello di maturità a vista d'occhio. C'è un'evoluzione costante che riguarda tutto il mondo dell'Internet of Things. I fornitori che propongono applicazioni IoT commerciali completamente funzionanti e integrate sono in numero crescente. Questo dimostra che l'IoT, oltre ad essere una tecnologia avanzata, si sta progressivamente trasformando in un vero e proprio servizio. Tuttavia, la sicurezza informatica resta una delle principali sfide ancora aperte, anche in considerazione del fatto che l'Internet delle Cose richiede una sicurezza su più livelli, coinvolgendo endpoint, rete e risorse cloud. Affrontare efficacemente questa sfida richiede che la sicurezza sia integrata sin dalle prime fasi del processo di progettazione.

Buona lettura!

Giordana Francesca Brescia

IoT Cyber Security

Founder&Editor
Emanuele Bonanni

CFO
Lidia Balica

Editorial Assistant
Maria Pisani

Maker in Chief
Giordana Francesca Brescia

Advertising & Marketing
Cristian Balica
cristian@contangosl.com

Graphic Designer
Marilde Mirra

Circulation
Users - 145.841
Social Network - 130.832

MICROCONTROLLORI E CRITTOGRAFIA

di **Daniele Valanzuolo**

La gestione della sicurezza dei dati e dei dispositivi elettronici è divenuta molto più critica e delicata dal momento in cui sono state integrate funzioni di interconnessione con il mondo esterno. Ogni nuovo progetto deve sempre fare i conti con gli aspetti di cyber-security affinché il dispositivo o il sistema in cui esso è inserito mantenga un adeguato livello di sicurezza. La lotta per la cyber-security purtroppo non è rimasta una questione vincolata soltanto a livello software, ma è stata recepita anche dai produttori dei dispositivi elettronici e dei microcontrollori. Di conseguenza, la tematica della cyber-security è diventata un argomento delicato anche per i progettisti hardware.

INTRODUZIONE

L'esponenziale sviluppo di prodotti tecnologici interconnessi, legati non solo all'ambito **IoT** domestico e consumer (smart device per la home, **wearable**, e via dicendo) ma anche ad ambiti più specifici e strategici come l'Industria 4.0 oppure i sistemi di sicurezza delle automobili, ha portato a doversi confrontare con gli aspetti di cyber sicurezza. Infatti, con l'evoluzione tecnologica sono evolute di pari passo anche le tecniche e le metodologie di attacco da parte degli hacker che, sfruttando le falle all'interno dei prodotti, possono prenderne il controllo e cambiare la logica di funzionamento del dispositivo. Fino a quando si tratta di gestire le luci di casa o il contapassi sul proprio smartwatch non vediamo complicazioni eccessive se non il fastidio di non disporre correttamente del dispositivo. Invece, se iniziamo a pensare ai dispositivi elettronici che gestiscono i sistemi più strategici quali gli impianti semaforici, il segnalamento delle linee ferroviarie ad alta velocità, le centraline di controllo di veicoli, navi o treni e via dicendo, capiamo come **tenere al sicuro il firmware** è di fondamentale importanza non solo per la disponibilità del servizio ma soprattutto per garantire la sicurezza delle persone. C'è da dire che **fino a qualche anno fa la tematica della cyber-security era un grattacapo focalizzato principalmente sulle righe di codice** e dunque sul software, soprattutto per quanto riguardava gli stack dei protocolli di comunicazione. Gli hacker prendevano di mira i sistemi entrando dalle falle dei firewall e colpivano installando dei software in grado di catturare informazioni sensibili. Tutto ciò avviene ancora oggi nella stragrande maggioranza dei casi, ma a questa metodologia di hackeraggio si sono aggiunte delle nuove tipologie di attacco che mirano ad upgradare e/o modificare il firmware dei dispositivi elettronici per poterne prendere il controllo.

IL RUOLO DELLA CRITTOGRAFIA

Nelle comunicazioni tra dispositivi interconnessi, come può essere il mondo dell'IoT, è fondamentale garantire la sicurezza dei messaggi trasferiti da un generico mittente al destinatario. La complessità della gestione della sicurezza cresce esponenzialmente con il numero di nodi che partecipano alla rete. Infatti, ogni nuovo nodo può essere un rischio potenziale per la rete. Man mano che i consumatori aumentano l'intelligenza e la connettività delle loro case, il rischio che gli hacker rubino i dati personali aumenta in modo esponenziale.
Con i dispositivi elettronici interconnessi, i rischi maggiori di attacco sono legati alle seguenti funzionalità:

- **Comunicazioni**: sono il principale canale di interfacciamento tra il dispositivo e il mondo esterno e questo avviene nella maggior parte dei casi attraverso canali non sicuri.
- **Procedure di aggiornamento firmware**: infatti, i microcontrollori di recente progettazione forniscono funzionalità avanzate per il caricamento dei firmware senza tool specifici di programmazione e soprattutto senza interconnessione diretta. Ovviamente, stiamo parlando della programmazione OTA (Over The Air) che ormai adotta qualsiasi produttore per poter garantire facilmente gli aggiornamenti agli utenti finali. Dunque, per poter garantire la sicurezza è fondamentale che i processi di caricamento del firmware di tipo OTA siano sicuri.
- **Porte di debug**

In tutte queste tipologie di attacco possiamo notare come il fattor comune capace di proteggere i dispositivi sia la crittografia.

IL PROBLEMA DELLE COMUNICAZIONI

Per garantire la sicurezza delle connessioni è necessario attuare **tecniche di autenticazione con chiavi di cifratura**. Il ricorso alle funzionalità di crittografia consente di poter ottenere comunicazioni più sicure anche su canali intrinsecamente non sicuri ed aperti a terzi. Le più diffuse tecniche di crittografia sono quelle a chiave simmetrica e a chiave pubblica. Nel primo caso, la sorgente e il destinatario utilizzano la stessa chiave che gli garantisce di poter eseguire le operazioni di cifratura e decifratura dei messaggi scambiati. Il vincolo principale è la conoscenza della chiave da tutti gli attori (sorgenti e destinatari) dei messaggi. Una volta scoperta la chiave, la comunicazione perde la sua sicurezza. I sistemi a chiave pubblica (Public Key Cryptographic) si basano su una coppia di chiavi di cui la prima è usata per la cifratura ed è pubblica mentre la seconda serve per decifrare il messaggio. Dunque, per poter garantire la sicurezza, quindi poter eseguire le operazioni di crittografia, è necessario adottare tecniche ad hoc per l'archiviazione sicura delle chiavi, la crittografia e l'autenticazione. L'esigua potenza di calcolo può rendere tali tecniche deboli e vulnerabili.

AGGIORNAMENTO DEL DISPOSITIVO IOT

Ormai quasi tutti i dispositivi interconnessi presentano funzionalità di aggiornamento da remoto (OTA o FOTA a seconda delle nomenclature scelte dai produttori). Un generico processo di aggiornamento del software o del firmware da remoto di dispositivi IoT prevede la ricerca ciclica degli aggiornamenti disponibili che verranno scaricati ed installati secondo le modalità scelte dal produttore o dall'utente finale. La procedura di update del firmware

sicuro includono sicuramente coprocessori per facilitare e semplificare l'utilizzo della crittografia e delle chiavi anche nelle fasi di upload del firmware. Ad esempio, le MCU della famiglia SAM D21 di **Microchip Technology** forniscono ai progettisti tecniche avanzate di aggiornamento OTA supportato da una specifica libreria di funzionalità in grado di verificare la presenza di nuovi firmware, gestirne il download, la verifica dell'integrità del firmware scaricato e il riavvio del dispositivo con il nuovo firmware.

Mentre inizialmente gli attacchi hardware prevedevano soltanto l'accesso fisico diretto al dispositivo (in linea generale alla porta di debug o di programmazione), oggigiorno risultano molto più evoluti in quanto possono essere condotti anche da remoto e portando al controllo o alla distruzione dell'unità attaccata. I microcontrollori tradizionali non presentano difese contro la maggior parte degli attacchi hardware. Per questo motivo, la maggior parte dei produttori ha ideato soluzioni ad hoc per migliorare il livello di sicurezza dei propri chip e fornire ai progettisti le risorse adeguate per garantire gli standard di sicurezza richiesti dalle specifiche applicazioni.

SOLUZIONI COMMERCIALI DISPONIBILI

Microchip fornisce microcontrollori con soluzioni di crittografia hardware conforme allo standard di sicurezza Device Identity Composition Engine (DICE) che consente l'operabilità con Microsoft Azure. Lo standard DICE nasce all'interno di un consorzio (DICE Architectures Work Group) con l'obiettivo di manutenere uno standard di requisiti e casi d'uso atti a definire una soluzione affidabile per garantire la sicurezza nelle comunicazioni. Il lavoro si concentra su una soluzione integrata hardware e software per poter ottenere funzionalità avanzate di crittografia con requisiti prestazionali minimi delle periferiche hardware. Lo standard DICE, essendo implementato già all'interno dell'hardware a disposizione, consente di garantire in ma-

L'IIOT COME VISIONE COMPLETA ALL'INTERNO DELLA CATENA DEL VALORE

di **Kontron**

Digitalizzazione, networking e IIoT stanno diventando sempre più importanti per le aziende che puntano ad aumentare la propria produzione o offrire nuovi servizi e prodotti digitali. Il viaggio da un progetto pilota IoT all'utilizzo popolare, tuttavia, è spesso difficile. Per tale motivo, Kontron sta intensificando i suoi sforzi per lanciare il suo set di strumenti software con il marchio kontron susietec.

I progetti di digitalizzazione relativi a **Industry 4.0, IIoT** e **AI** (**Artificial Intelligence**) prosperano grazie al collegamento in rete di tutte le risorse, alla **tecnologia dei sensori** e all'integrazione di un'ampia varietà di **dati**. In pratica, ci sono molti proof of concepts e progetti pilota; tuttavia, questi argomenti non sono stati ancora ampiamente implementati nella maggior parte delle aziende. Ciò è dovuto anche all'approccio tramite progetti individuali. Invece di concentrarsi sui progetti, l'attenzione dovrebbe essere focalizzata sui processi: l'installazione di un dispositivo che misuri i dati di temperatura non fa parte di una visione IoT. **La soluzione non è più solo l'hardware**, motivo per cui i produttori devono in futuro integrare i loro portafogli di prodotti con software e competenze.

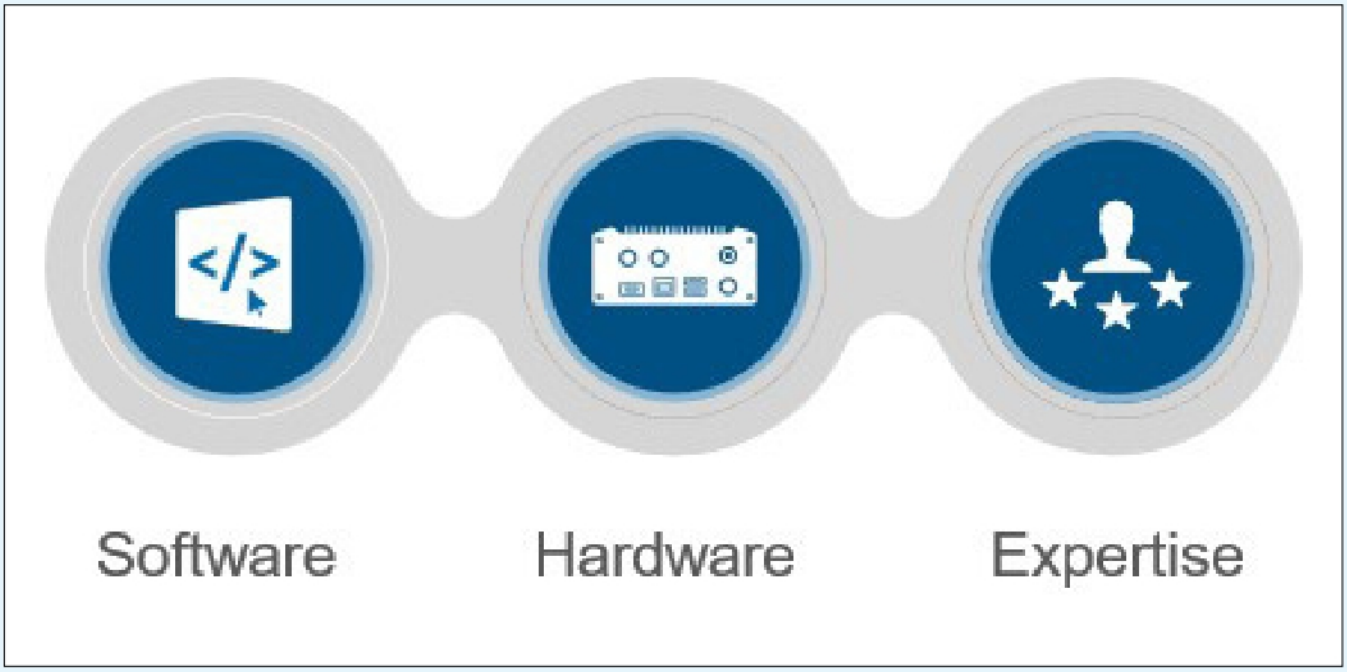
È RICHIESTA UNA MENTALITÀ PRATICA

Il networking, tuttavia, è un'importante sfida preliminare che deve essere superata. È qui che sono necessari partner con know-how industriale che abbiano familiarità con le competenze spesso complesse che circondano il controllo e l'automazione e che siano disposti a dare una mano invece di nascondersi dietro una visione unica. Quando si tratta di trarre vantaggio dal networking e dall'analisi dei dati, l'attenzione è spesso rivolta ai processi end-to-end che attraversano intere catene del valore. È, pertanto, di scarsa utilità se un solo reparto assume l'incarico. La maggior parte degli argomenti sono interdisciplinari: l'intera azienda dovrà evolversi. Pertanto, sono essenziali il giusto assetto e il coinvolgimento di persone di tutti i reparti. Inoltre, la moltitudine di argomenti e di partecipanti rende la gestione dei progetti estremamente impegnativa. La digitalizzazione è in definitiva un processo completo che consiste in una serie di singoli progetti. Il software intorno all'IIoT, tuttavia, ha un profondo impatto sui processi aziendali. Nuovi problemi complessi possono sorgere senza obiettivi chiari da parte del management aziendale. Ciò è particolarmente vero quando si tratta di raccolta ed elaborazione dei dati.

UN UNICO SET DI STRUMENTI PER TUTTI GLI SCENARI IIOT

Diversi approcci alla digitalizzazione si basano su differenti sensori, macchine o dispositivi, nonché sui loro dati. Per evitare di riprogettare il ciclo in ogni contesto, **Kontron** ha sviluppato un set di strumenti composto da hardware, software e competenze che possono essere ampliate in base alle esigenze, aumentando con le crescenti richieste all'interno dell'azienda.

Il set di strumenti **kontron susietec** consente di implementare quasi tutti gli scenari applicativi IIoT nell'industria. La stretta **integrazione dello sviluppo software e hardware** nel gruppo **Kontron** è un grande vantaggio: in particolare, per le applicazioni real-time, è importante che l'hardware come i gateway o altri dispositivi edge e il software corrispondente siano allineati in modo coerente tra loro. Nell'ambiente dell'**Intelligenza Artificiale**, gli algoritmi spesso vengono eseguiti nell'edge, ad esempio



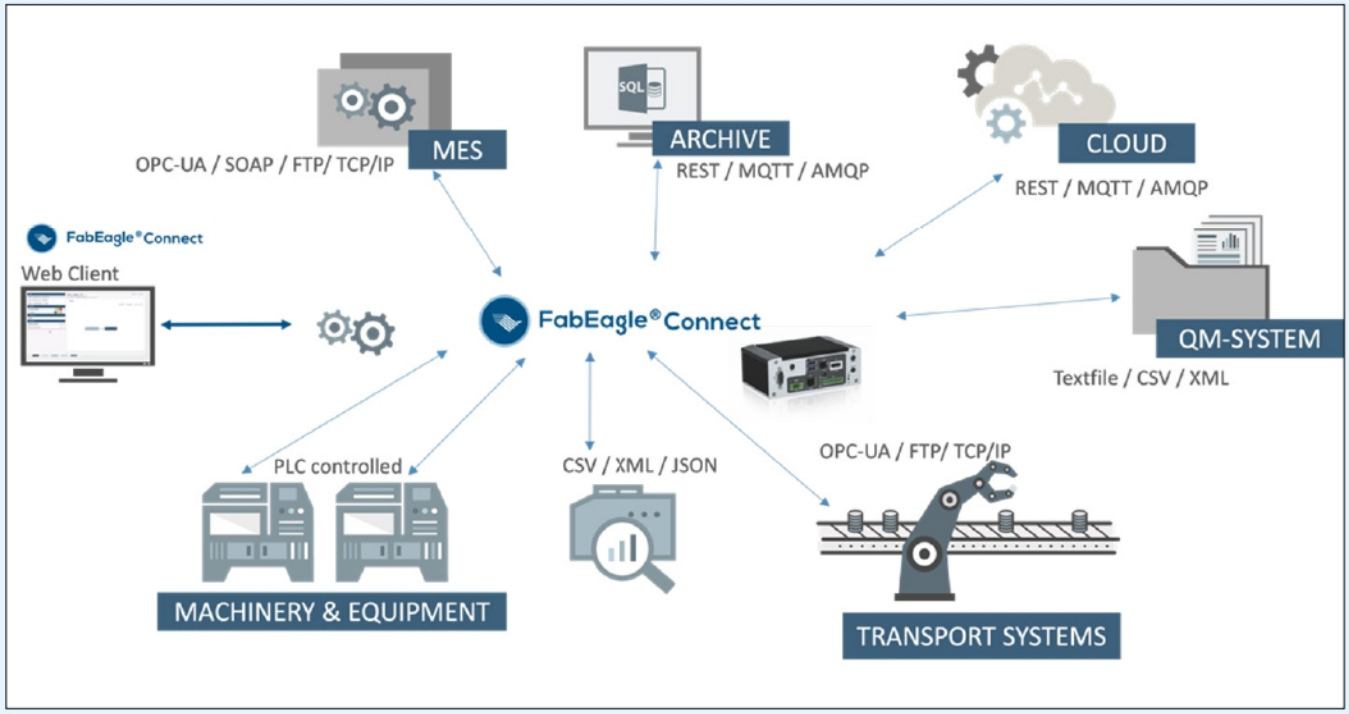
nel controllo qualità automatizzato basato sulla visione artificiale nella produzione. Di conseguenza, in questo settore stanno acquisendo importanza soluzioni software e hardware coordinate. Anche qui è evidente una crescente domanda di calcolo ad alte prestazioni (**HPC, High-Performance Computing**).

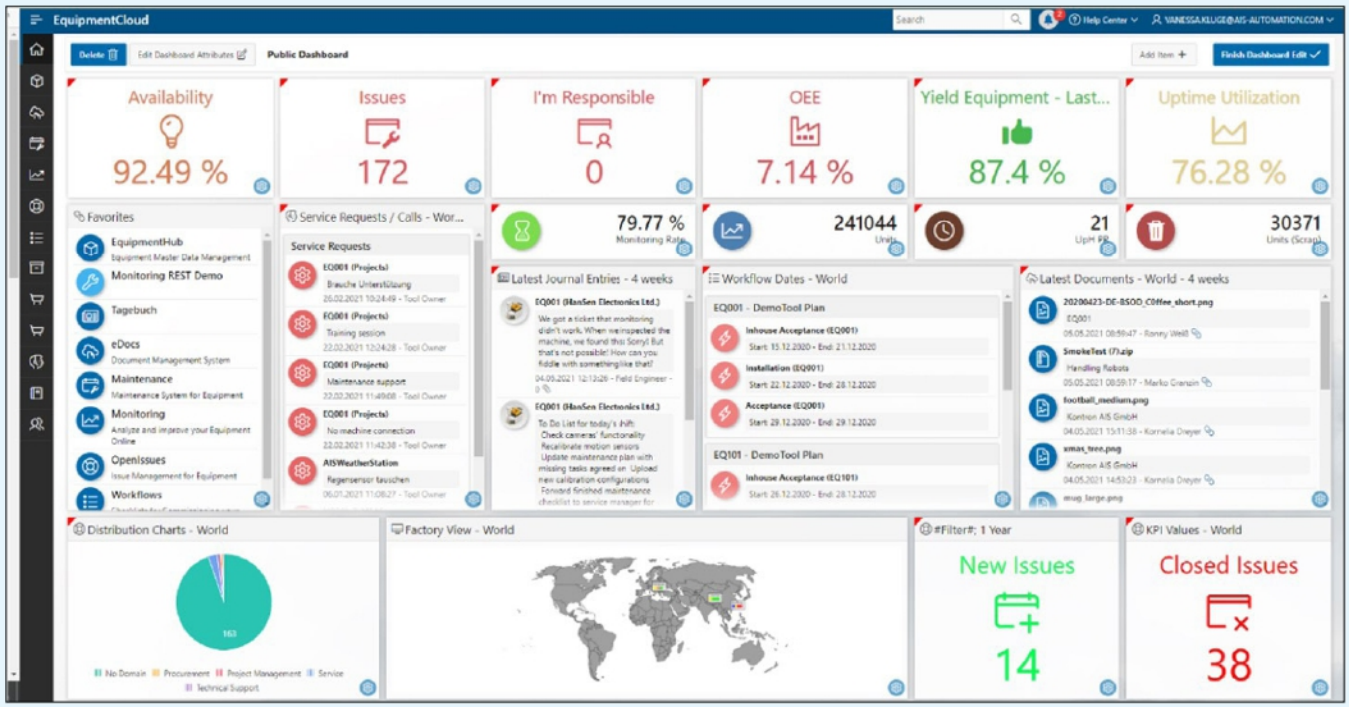
MINIMIZZARE I PROBLEMI DI INTERFACCIA

Solo i dati selezionati di macchine e sensori dovrebbero migrare al cloud, non solo per motivi di latenza e sicurezza, ma anche per evitare il sovraccarico della rete. Ciò significa che i dati devono essere pre-elaborati all'edge e resi disponibili per diverse applicazioni in infrastrutture ibride. Ciò richiede un middleware in grado di memorizzare nella cache i dati per aumentarli con timestamp, aggregarli, comprimerli o convertirli. Solo allora le informazioni diventano utilizzabili e confrontabili per l'analisi dei dati.
Allo stesso tempo, il toolset susietec fornisce un contributo significativo nel padroneggiare i problemi di interfaccia che causano regolarmente molto lavoro sul campo. La maggior parte dei dati provenienti dai controller e dai sensori viene generalmente utilizzata per il controllo di processo nella connessione dei sistemi integrati nella catena di processo. Sulla base dell'esperienza, molti progetti richiedono anche una connessione tra il sistema di controllo della produzione e un sistema ERP. Come piattaforma di connettività, il toolset susietec fornisce funzionalità di sicurezza coerenti e raggruppa tutte le interfacce in modo trasparente. È già disponibile un gran numero di interfacce standardizzate, per cui sono necessari solo piccoli aggiustamenti durante l'integrazione di nuovi sistemi.

STEP BY STEP, MA CON UN PROGRAMMA

Invece di investire in una soluzione enorme con elementi in eccesso, le aziende dovrebbero essere in grado di utilizzare esattamente i componenti del set di strumenti susietec necessari per l'applicazione in questione. Questi possono includere approcci di automazione nella produzione, temi di controllo nel back office, ottimizzazioni nel servizio sul campo o app per visualizzare e ottimizzare i processi. La digitalizzazione è semplice. Le singole applicazioni sono interconnesse in modo tale che le aziende possano creare un panorama IoT continuo e integrato e adattarlo step by step per soddisfare i nuovi requisiti.
L'approccio step by step è illustrato, ad esempio, da un progetto pratico nella costruzione di macchine special-purpose: l'attività iniziale era quella di valutare i messaggi di errore e stabilire le basi per la manutenzione predittiva. I tecnici dell'assistenza hanno quindi ricevuto messaggi sui loro tablet o smartphone subito dopo. Infine, è stato aggiunto un modulo che gestisce l'intera pianificazione dell'implementazione, il coordinamento degli appuntamenti, la gestione delle parti di ricambio e il supporto on-site. Nuove esigenze del settore sorgono spesso nel tempo, non appena vengono riconosciuti il valore aggiunto e le possibilità del networking. Tuttavia, è fondamentale esaminare attentamente i concetti di **Intelligenza Artificiale** e **Machine Learning**, ad esempio, e portare le com-

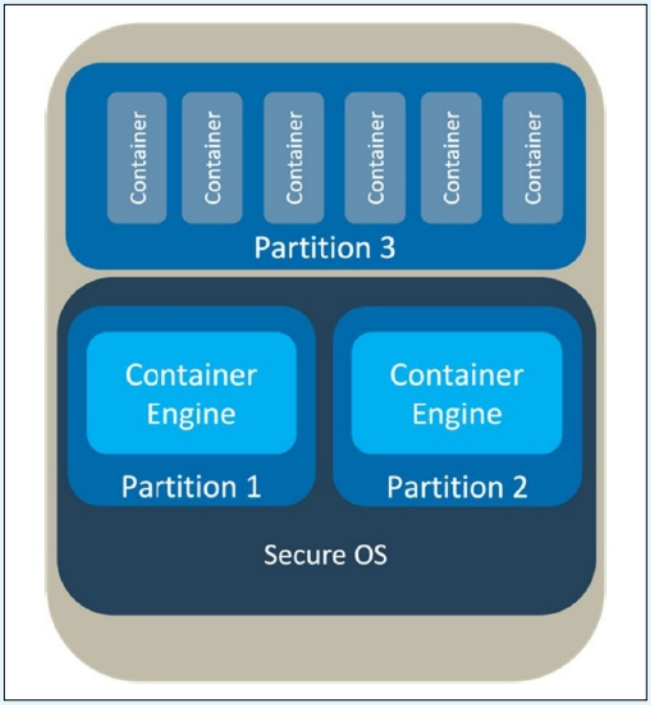




petenze a bordo. Il diavolo sta nei dettagli e non tutte le possibilità applicative dell'IA possono essere implementate economicamente.

LA MANUTENZIONE DA REMOTO RICHIEDE SOLUZIONI INTEGRATE

Vi è una tendenza generale all'acquisizione di importanza dei servizi digitali, soprattutto nell'area della costruzione di macchine e impianti così come nella manutenzione. Per questo motivo, le **soluzioni IIoT** dovrebbero consentire un accesso sicuro tramite un portale di terze parti, ad esempio per i tecnici dell'assistenza presso la sede del cliente. Possono essere inoltrati avvisi e analisi relativi alla manutenzione predittiva o all'ottimizzazione della macchina. Esiste un notevole potenziale di efficienza nel settore della telegestione per la diagnosi e la manutenzione a



distanza. Tuttavia, anche con questo topic, a prima vista chiaramente gestibile, devono essere superati numerosi ostacoli, come i firewall e specifici requisiti di sicurezza presso l'ubicazione di macchine e impianti. In questo senso, i normali tool commerciali raggiungono rapidamente limiti che non possono essere superati efficacemente.
Gli scenari IIoT sono in genere altamente individuali: ogni caso d'uso ha configurazioni differenti. Solo alcuni dati devono essere archiviati e trasmessi a sistemi diversi in ciascun caso. Ad esempio, se le macchine vengono noleggiate con un modello pay-per-use, i dati sui tempi di funzionamento devono essere disponibili centralmente nel cloud. Tuttavia, se il servizio offerto è solo di manutenzione, questi dati non sono necessari nel cloud. La gestione dei dati su misura per il rispettivo caso d'uso è fondamentale.

IL SECURITY BY DESIGN È FONDAMENTALE NELL'INDUSTRIA

La vulnerabilità di un numero sempre maggiore di sistemi aperti nella produzione industriale sta aumentando ogni anno, come dimostrano in modo impressionante le cifre dei report del German Federal Office for Information Security sulla situazione annuale. Il BSI consiglia strategie che iniziano con la **sicurezza nel processo di progettazione**.
Per l'ambiente IIoT, ciò significa che il software deve già fare la differenza configurando un sistema operativo sicuro individualmente per l'applicazione e mantenendolo coerentemente con le patch di sicurezza regolari. Le richieste e i canali di comunicazione sono molto diversi in questo settore. I sistemi operativi standard, d'altra parte, spesso devono essere adattati alla rispettiva situazione con notevoli sforzi di configurazione e manutenzione. Inoltre, le prestazioni del sistema sono spesso sovraccaricate di funzionalità di sicurezza a tal punto che i dispositivi non possono più svolgere la loro funzione effettiva al meglio delle loro capacità. Per tale ragione, l'utilizzo del SecureOS di susietec diventa vantaggioso non appena ci sono un certo numero di dispositivi nel campo.

IL TOOLSET KONTRON SUSIETEC

Con susietec, **Kontron** offre un set di strumenti che copre tutti gli aspetti della gestione dei dispositivi, della gestione remota e dell'edge computing. Sono inclusi anche la gestione dei dati e l'elaborazione dei dati in tempo reale, l'IA, l'apprendimento automatico e l'analisi. Questo toolbox che comprende software, hardware coordinato e competenze consente, tra le altre cose, lo sviluppo semplice di app e dashboard intelligenti in modo che le aziende possano beneficiare di nuovi servizi basati sui dati.

INTERVISTA

Perché molte aziende lottano ancora con il networking digitale della loro produzione e con i profitti derivanti dai dati?

Il compito della digitalizzazione è ottimizzare i flussi di lavoro esistenti e stabilire nuovi processi efficienti, che fino ad oggi erano tecnologicamente irrealizzabili. L'obiettivo di tutto questo è migliorare le prestazioni di un'azienda e attrezzarla per le esigenze future.
La digitalizzazione è in definitiva un processo che consiste in molti progetti più piccoli e che deve coinvolgere molti partecipanti.
I progetti di digitalizzazione relativi a Industry 4.0, IIoT e AI prosperano grazie al collegamento in rete di tutte le risorse, alla tecnologia dei sensori e all'integrazione di un'ampia varietà di dati.
Il networking, spesso anche attraverso il retrofit di macchine e sistemi, è un primo grande ostacolo da superare. In questo caso è di scarsa utilità se solo un reparto si mette all'opera, perché la maggior parte delle questioni sono interdisciplinari, in altre parole, l'intera azienda ha bisogno di evolversi.
A tal fine, i dipendenti di tutti i reparti coinvolti dovrebbero entrare a far parte del processo.

In che modo la trasformazione digitale e l'IIoT cambieranno le cose?

La trasformazione digitale permea tutte le strutture, fino ai singoli processi lavorativi o al modo in cui vengono svolte le attività; fino al modello di business, che si adatta o cambia in modo abbastanza drammatico. Affinché la trasformazione abbia successo, è quindi importante comprendere la dimensione di questi problemi tecnologici sin dall'inizio, non sottovalutarli cronicamente o evitarli per paura. Molte cose vanno di pari passo; ad esempio, un approccio più innovativo si traduce in progetti e metodi di lavoro diversi come Scrum o DevOps, con la scomparsa delle gerarchie e lo spostamento della responsabilità sui team esecutivi interfunzionali. Nel processo, molte posizioni stanno cambiando in modo significativo, soprattutto a livello di gestione.

Quali sono i problemi tipici legati all'introduzione di queste tecnologie?

Questa trasformazione inizia spesso nei reparti di ricerca e sviluppo. Tuttavia, in quest'area prevale una visione molto tecnica: le aziende pensano in termini di dispositivi e quali dati possono essere raccolti con essi. Tuttavia, il vero problema sono gli obiettivi di business e una visione per il futuro, che devono provenire dal consiglio di amministrazione. Dove vuoi essere tra cinque anni? I fornitori di servizi esterni possono supportare qui e indicare le possibilità, ma questo orientamento è qualcosa che dovrebbe provenire dall'azienda stessa. Tuttavia, questo messaggio e la comprensione dei principali cambiamenti resi possibili dall'IIoT e dall'IA non hanno ancora raggiunto tutti i livelli esecutivi da molto tempo. Aggrapparsi allo status quo, soprattutto quando l'azienda ha attualmente un discreto successo, e le solite forze di inerzia prevalgono ancora in molte aziende.

Perché una strategia onnicomprensiva e il necessario know-how sono così importanti nell'ambiente IIoT?

Il software nel contesto dell'IIoT ha un profondo impatto sui processi aziendali. Senza un obiettivo chiaro, l'implementazione dei singoli progetti è praticamente come volare alla cieca. In particolare, quando si parla di nuovi servizi digitali e modelli di business, per trovare una visione è necessaria anche una consulenza che fornisca informazioni sugli aspetti economici. Ad esempio, in che modo si collegano i costi di un'idea alle possibilità di monetizzazione? Al di là di queste considerazioni strategiche, le aziende si trovano ad affrontare anche un'enorme carenza di qualificati analisti di dati. I fornitori di hardware e servizi di integrazione devono quindi anche fornire ulteriore supporto per la scienza dei dati.

Quando si parla con esperti di networking, diventa ogni volta chiaro: il tema del retrofitting si avvicina in pratica a una "strage"; molte cose sono estremamente piccole. Quindi in che modo può essere ancora raggiunto ciò?

Abbiamo un team dedicato con anni di esperienza nel retrofitting e andiamo direttamente alla linea di produzione per far funzionare le soluzioni lì. È anche importante che l'hardware, il software e le competenze siano perfettamente abbinati. È qui che abbiamo un vantaggio decisivo grazie alla stretta collaborazione tra lo sviluppo software e hardware all'interno del gruppo **Kontron**. La sfida principale è mantenere una visione d'insieme, non impantanarsi e selezionare le azioni giuste al momento giusto: concetti IoT più ampi di solito coinvolgono molti siti progettuali. Soprattutto perché molte persone diverse o gli stakeholders sono quindi coinvolti in tali progetti, una gestione efficiente è estremamente importante.

Si ringrazia, per la collaborazione con Elettronica Open Source, Bernhard Günthner, Executive Vice President IoT Software, Kontron AG.

L'autore è a disposizione nei commenti per eventuali approfondimenti sul tema dell'Articolo. Di seguito il link per accedere direttamente all'articolo sul Blog e partecipare alla discussione:
https://it.emcelettronica.com/liiot-come-visione-completa-allinterno-della-catena-del-valore

COME MIGLIORARE LE MISURE DI CORRENTE A LIVELLO DI SISTEMA CON I MODULATORI ISOLATI SIGMA-DELTA DI PROSSIMA GENERAZIONE

di **Analog Devices**

Questo articolo introdurrà innanzitutto la specifica relativa all'immunità ai transitori di modo comune (CMTI) e la sua importanza in un sistema. Verrà discussa una nuova famiglia di modulatori sigma-delta isolati, le relative prestazioni e come questi facilitino le misure di corrente del sistema e ne migliorino l'accuratezza, in particolare per quanto riguarda l'errore di offset e la sua deriva. Infine, verrà presentata una soluzione circuitale consigliata allo scopo.

INTRODUZIONE

I modulatori isolati sono ampiamente utilizzati su motori/inverter per i quali si richiede un'elevata precisione di misura della corrente e isolamento galvanico. Con la rivoluzione dovuta all'alto livello di integrazione e l'elevata efficienza nei sistemi motore/inverter, i FET SiC e GaN stanno iniziando a sostituire i MOSFET e gli IGBT grazie alle loro dimensioni ridotte, alla frequenza di commutazione più alta e ai vantaggi offerti da un dissipatore di calore più piccolo. Tuttavia, per i componenti di isolamento è necessaria un'elevata capacità CMTI. È inoltre necessaria una misura di corrente di accuratezza maggiore. Il modulatore isolato di nuova generazione aumenta notevolmente la capacità CMTI e migliora la precisione.

COS'È L'IMMUNITÀ AI TRANSITORI DI MODO COMUNE?

L'immunità ai transitori di modo comune (CMTI, Common Mode Transient Immunity) specifica la velocità di salita e discesa di un impulso transitorio applicato attraverso la barriera isolante, oltre la quale vengono corrotti i segnali di clock o dati. Vengono registrate sia la velocità di variazione che la tensione assoluta di modo comune (VCM) dell'impulso.

I nuovi modulatori di isolamento sono stati testati in condizioni di CMTI statiche e dinamiche. Il test statico rileva gli errori a singolo bit del dispositivo. I test dinamici monitorano l'uscita dei dati filtrati per verificare le variazioni nelle prestazioni di rumore in seguito a un'applicazione randomizzata dell'impulso CMTI. La **Figura 1** mostra uno schema a blocchi dettagliato del test.

Il CMTI è importante perché i transitori con alto slew rate (alta frequenza) possono corrompere la trasmissione dei dati attraverso la barriera isolante. Comprendere e misurare la sensibilità a questi impulsi transitori è fondamentale. I metodi di prova di ADI si basano sullo standard IEC

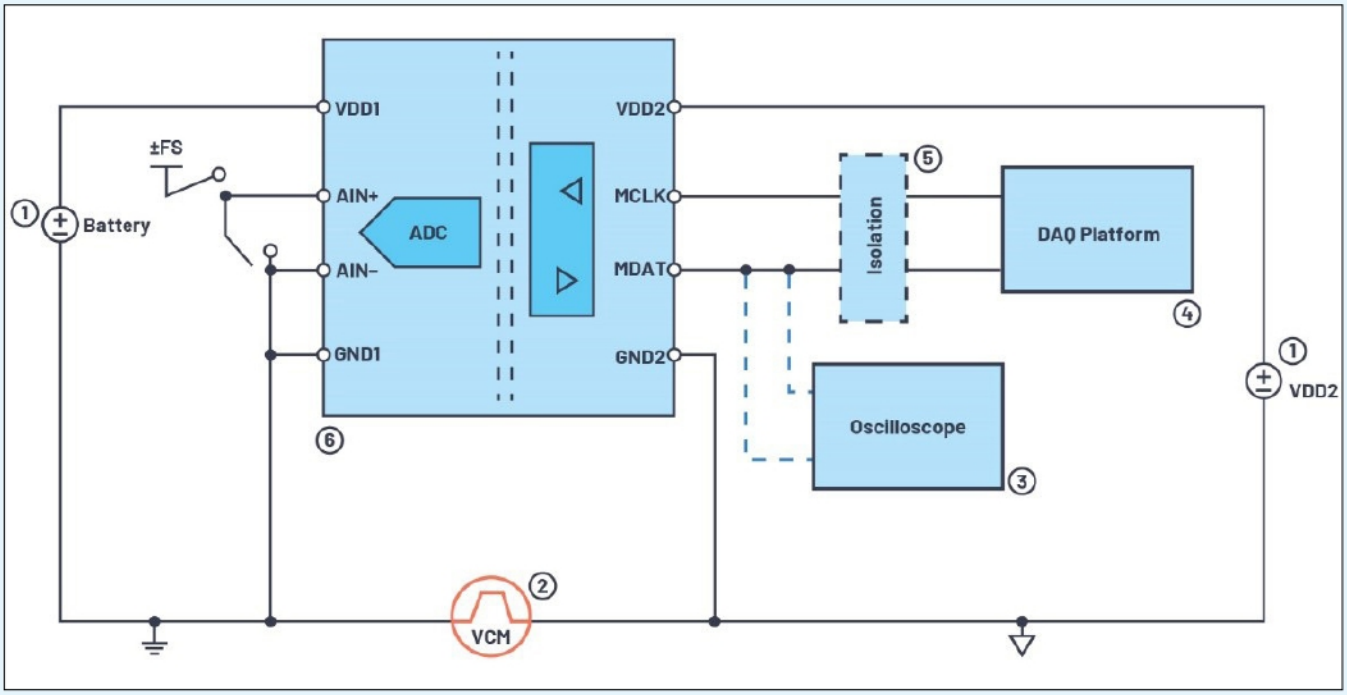


Figura 1: Schema a blocchi semplificato del test CMTI

60747-17, che riguarda le modalità di misura dell'immunità ai transitori di modo comune (CMTI) per gli accoppiatori magnetici.

COME CARATTERIZZARE IN LABORATORIO IL CMTI PER UN MODULATORE ISOLATO

La piattaforma di prova CMTI illustrata in **Figura 1** include i seguenti componenti:

- Alimentazione a batteria per VDD1/VDD2.
- Un generatore di impulsi di modo comune ad alta tensione.
- Un oscilloscopio per monitorare i dati.
- Una piattaforma di acquisizione dati per la relativa analisi e un filtro sinc3 per la decimazione 256 usato per un modulatore isolato.
- Un modulo di isolamento (di solito si usa l'isolamento ottico).
- Un modulatore isolato.

Per il test CMTI statico e dinamico si utilizza la stessa piattaforma, variano soltanto i segnali di ingresso. Questa piattaforma può essere utilizzata anche per testare le prestazioni CMTI di altri prodotti isolati. Nel caso dei modulatori isolati, il flusso di dati one-bitstream viene decimato e filtrato, per essere poi trasferito al loop di controllo del sistema di gestione del motore, per cui il test dinamico CMTI risulterà più completo e utile. La **Figura 2** e la **Figura 3** mostrano le prestazioni del test dinamico CMTI nel dominio del tempo e della frequenza con diversi livelli di CMTI. Dalla **Figura 2** si può notare che lo spur diventa più grande quando si aggiunge un segnale transitorio VCM più elevato per lo stesso modulatore isolato. Quando il segnale transitorio VCM supera le specifiche del modulatore isolato, nel dominio del tempo appare uno spur molto pronunciato (come indicato nella **Figura 2c**). Questo ha gravi conseguenze nell'utilizzo di un sistema di controllo per motori, provocando un ripple considerevole sulla coppia.
La **Figura 3** mostra le prestazioni nel dominio FFT in presenza di diversi transitori in frequenza (il che significa mantenere costante l'ampiezza del segnale VCM modificando invece il periodo del transitorio stesso). I risultati della **Figura 3** mostrano che le armoniche sono strettamente correlate alla frequenza del transitorio. Pertanto, maggiore è la capacità CMTI del modulatore di isolamento, minore è il livello di rumore nell'analisi FFT. Rispetto ai modulatori isolati di generazione precedente, la prossima generazione di dispositivi ADuM770x aumenta la capacità CMTI da 25 kV/µs a 150 kV/µs, migliorando notevolmente l'immunità ai transitori del sistema, come illustrato nei dati di confronto riportati nella **Tabella 1**.

TECNICA DI COMPENSAZIONE E CALIBRAZIONE A LIVELLO DI SISTEMA

In un sistema di controllo motore o inverter, maggiore è l'accuratezza dei dati sui valori di corrente, più stabile ed efficiente è il sistema. Offset e guadagno sono fonti di

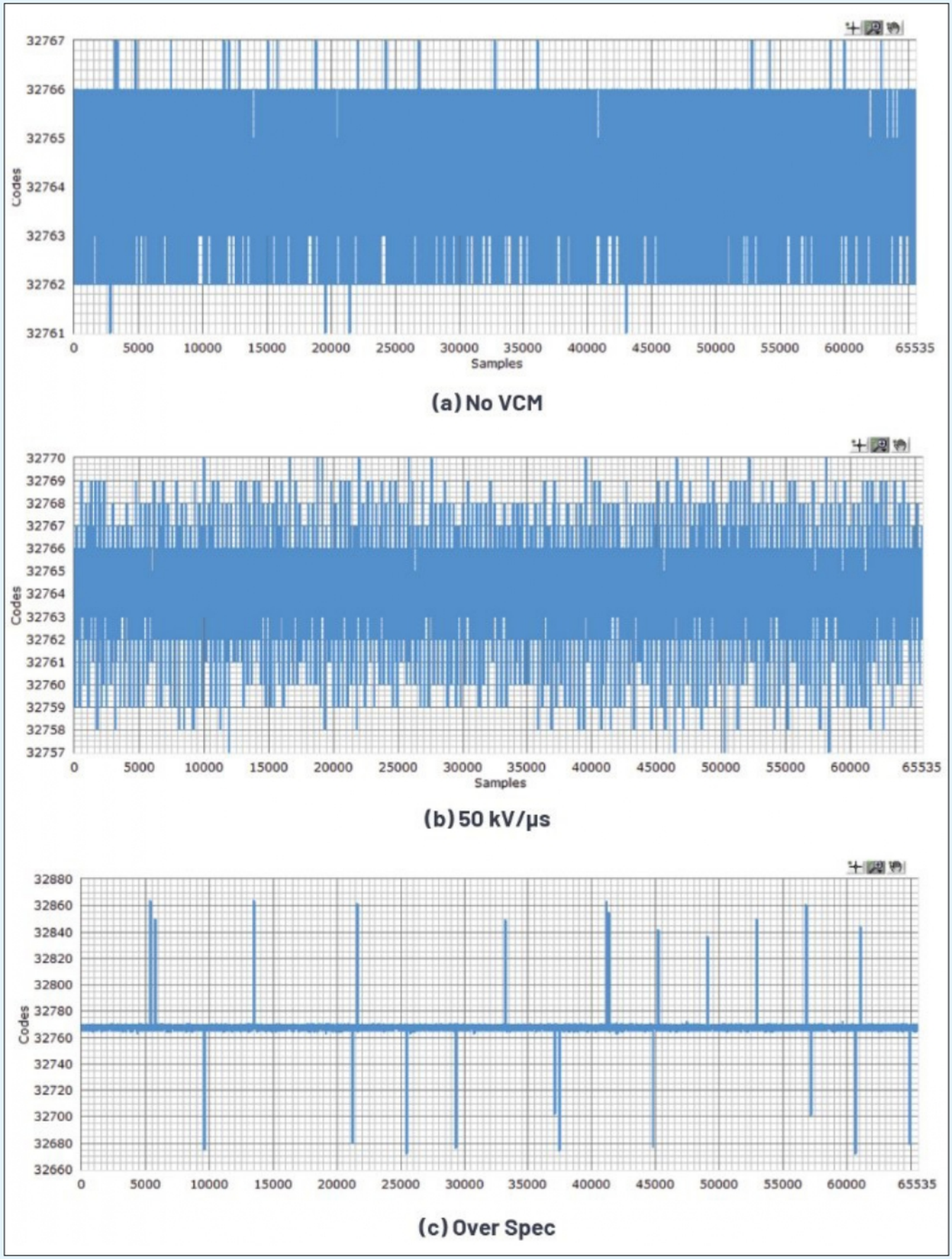


Figura 2: Prestazioni del test CMTI dinamico nel dominio del tempo

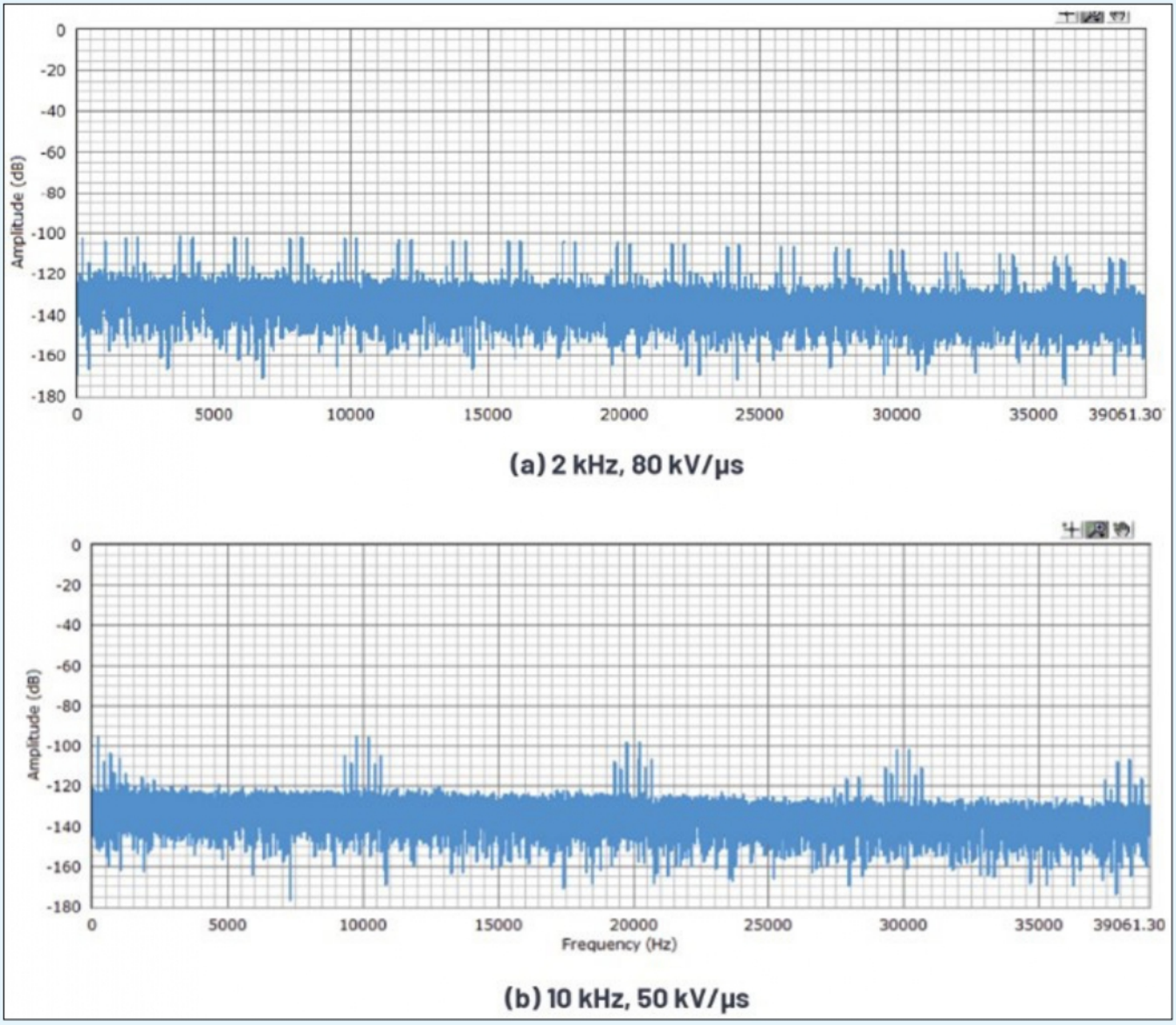


Figura 3: Prestazioni del test CMTI dinamico nel dominio della frequenza

errore DC piuttosto comuni negli ADC. La **Figura 4** mostra come gli errori di offset e di guadagno influenzino la funzione di trasferimento dell'ADC. In un sistema, questi errori possono manifestarsi sotto forma di ripple di coppia o di velocità. Per limitare il loro impatto nella maggior parte dei sistemi, questi errori possono essere calibrati a temperatura ambiente.

Al contrario, la deriva dell'offset e gli errori di guadagno sull'intero intervallo di temperatura costituiscono un problema, poiché sono più difficili da compensare. A condizione che la temperatura del sistema sia nota, per i convertitori con profili di deriva lineari e prevedibili la compensazione degli errori di offset e guadagno da deriva termica è possibile (anche se è costosa e richiede tempo), aggiungendo un fattore di compensazione al profilo di deriva dell'offset per renderlo il più piatto possibile. Questo metodo di compensazione dettagliato è descritto nella nota applicativa AN-1377. Esso può ridurre il valore di deriva specificato nei data sheet di AD7403/AD7405 fino al 30% per l'offset e fino al 90% per il guadagno, e può essere applicato a qualsiasi altro componente del convertitore quando si desidera migliorare l'errore da deriva termica di offset e guadagno a livello di sistema.

COME SI UTILIZZA LA TECNICA DI "CHOPPING"

In alternativa, per un progettista di sistemi può risultare più efficiente e conveniente usare una tecnica chiamata "chopping", che può anche essere integrata efficacemente nel silicio stesso per ridurre al minimo gli errori di deriva

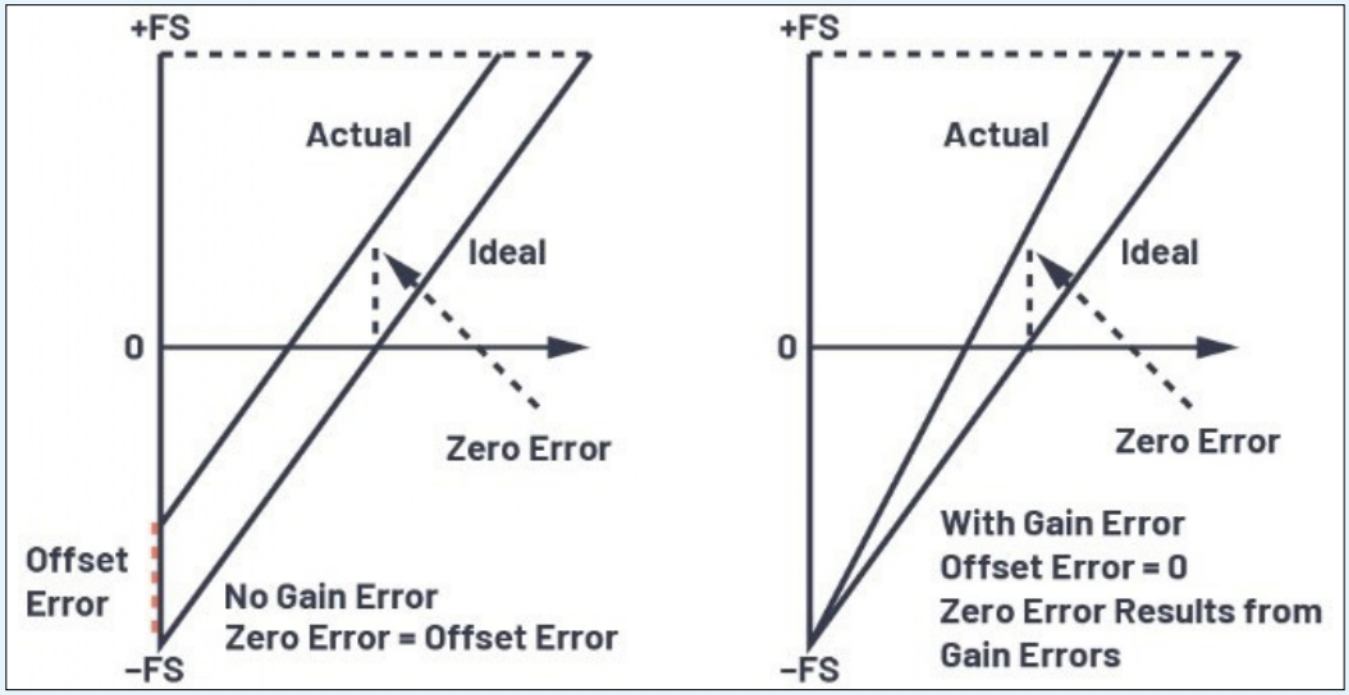


Figura 4: Errore di offset e di guadagno nella funzione di trasferimento di un ADC

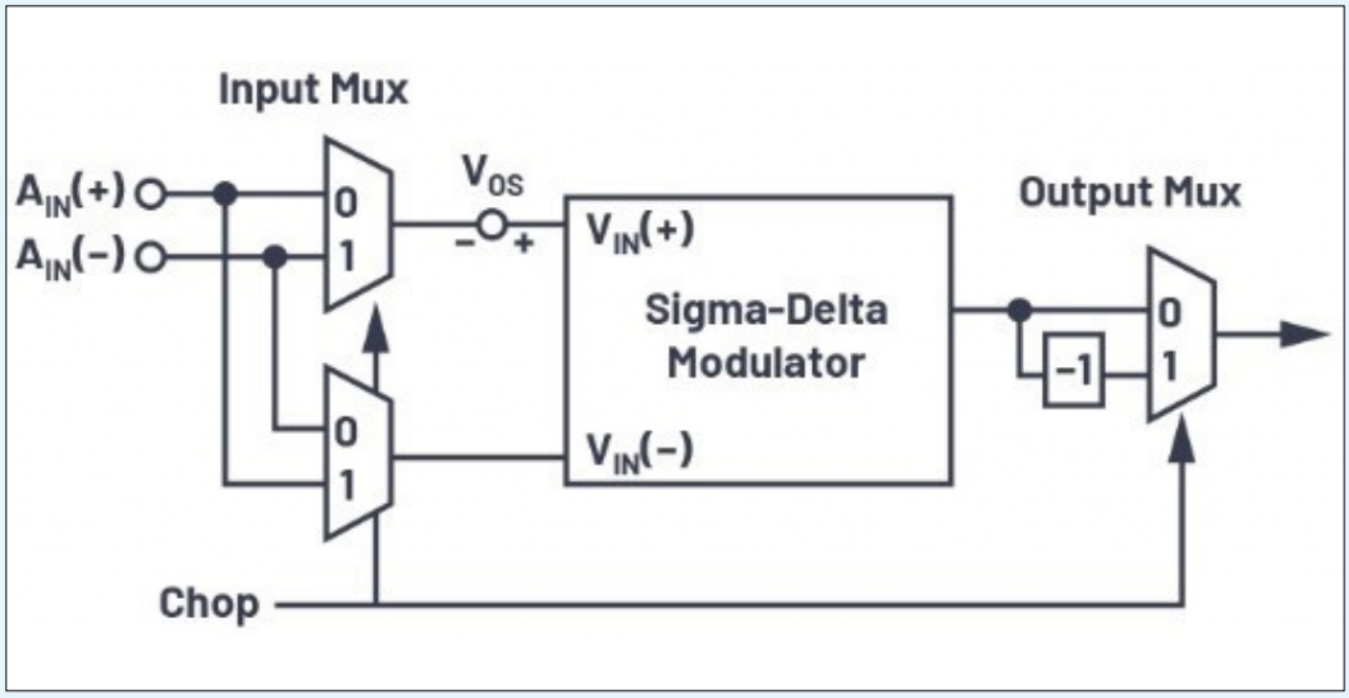


Figura 5: Chopping

di offset e guadagno. Lo schema del chopping è illustrato nella **Figura 5**, dove la soluzione implementata su un ADC consiste nell'intervenire sull'intera catena del segnale analogico per eliminare ogni errore di offset e di bassa frequenza.

L'ingresso differenziale al modulatore viene alternativamente invertito ("chopped") dal multiplexer d'ingresso e per ogni fase di "chop" viene eseguita una conversione ADC (commutando il mux allo stato "0" o "1"). Prima di passare il segnale di uscita al filtro digitale, il chopping del modulatore viene invertito nel multiplexer di uscita.

Se l'offset nel modulatore sigma-delta è rappresentato come V_{OS}, l'uscita è $(A_{IN}(+) - A_{IN}(-)) + V_{OS}$ quando il chop è 0 e l'uscita è $-[(A_{IN}(-) - A_{IN}(+)) + V_{OS}]$ quando il chop è 1.

Specifica Principale		ADuM7701/ ADuM7703	ADuM7702/ ADuM7704	AD7403	AD7401
Isolamento	Tensione Nominale (V_{PK})	1270	1270	1250	891
	CMTI (kV/µs) (min)	150	150	25	25
Prestazione	Errore di Offset (mV max)	±0,18	±0,18	±0,75	±0,6
	Deriva di Offset (µV/°C max) a 50 mV	—	±0,25 (16-pin) ±0,6 (8-pin)	—	—
	Deriva di Offset (µV/°C max) a 250 mV	±0,6	—	3,8	3,5
	Errore di Guadagno (%FSR max)	±0,2	±0,2	±1,2	±0,3
	Deriva di Guadagno (ppm/°C) a 50 mV	—	±15,6 (typ) ±31,3 (max)	—	—
	Deriva di Guadagno (ppm/°C) a 250 mV	±12,5 (typ) ±28 (max)	—	65 (typ) 95 (max)	36 (typ)
	ENOB (bit) a 50 mV	14,2 (typ) — 13,1 (min)		—	—
	ENOB (bit) a 250 mV	14 (typ) 13,3 (min)	—	14.2 (typ) 13,1 (min)	11,5 (typ)
Integrazione	LDO	No	Si	No	No
Package		8-pin e 16-pin	8-pin e 16-pin	8-pin e 16-pin	16-pin

Tabella 1: Confronto delle Specifiche Principali

La tensione di errore, V_{OS}, viene rimossa mediando questi due risultati nel filtro digitale, ottenendo (A_{IN} (+) - A_{IN} (-)), che equivale alla tensione differenziale di ingresso senza alcuna componente di offset.

L'ultimo modulatore isolato rilasciato da ADI migliora le prestazioni relative all'errore di offset e di guadagno grazie all'ottimizzazione del circuito analogico interno e utilizzando la più recente tecnica di chopping, che semplifica

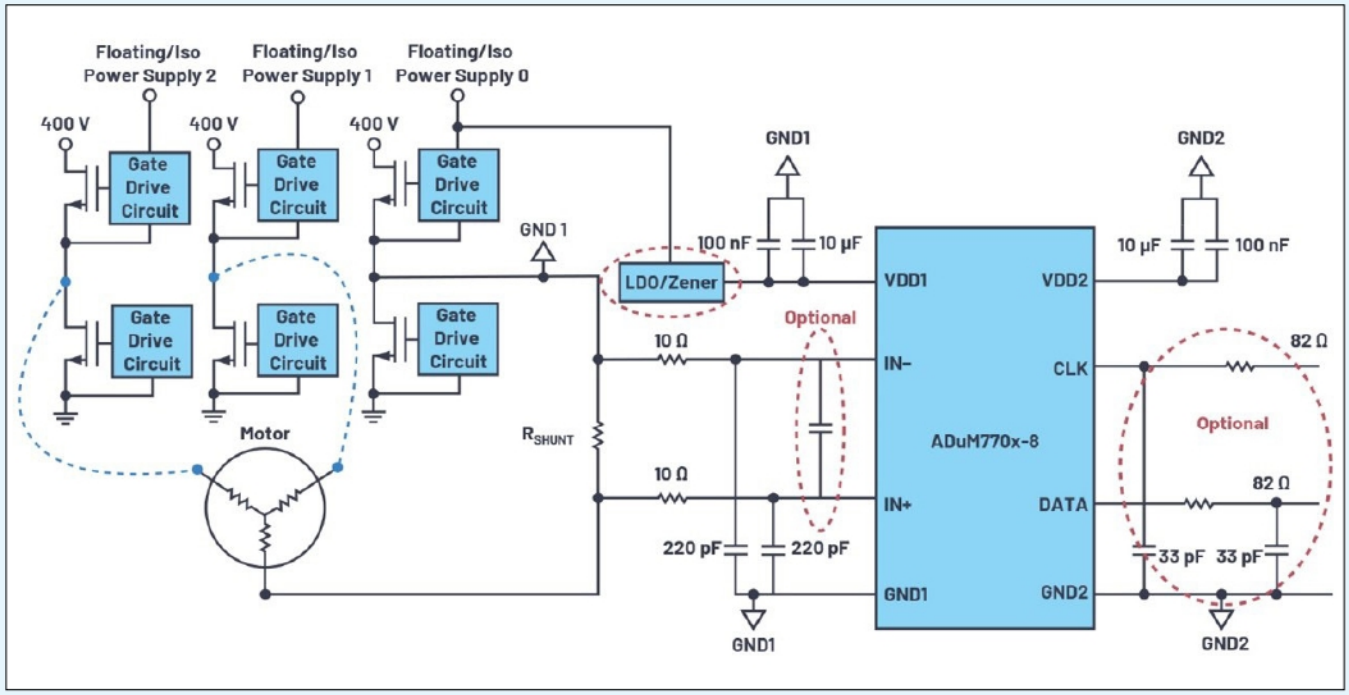


Figura 6: Circuito tipico per la misura della corrente in un sistema di controllo motore

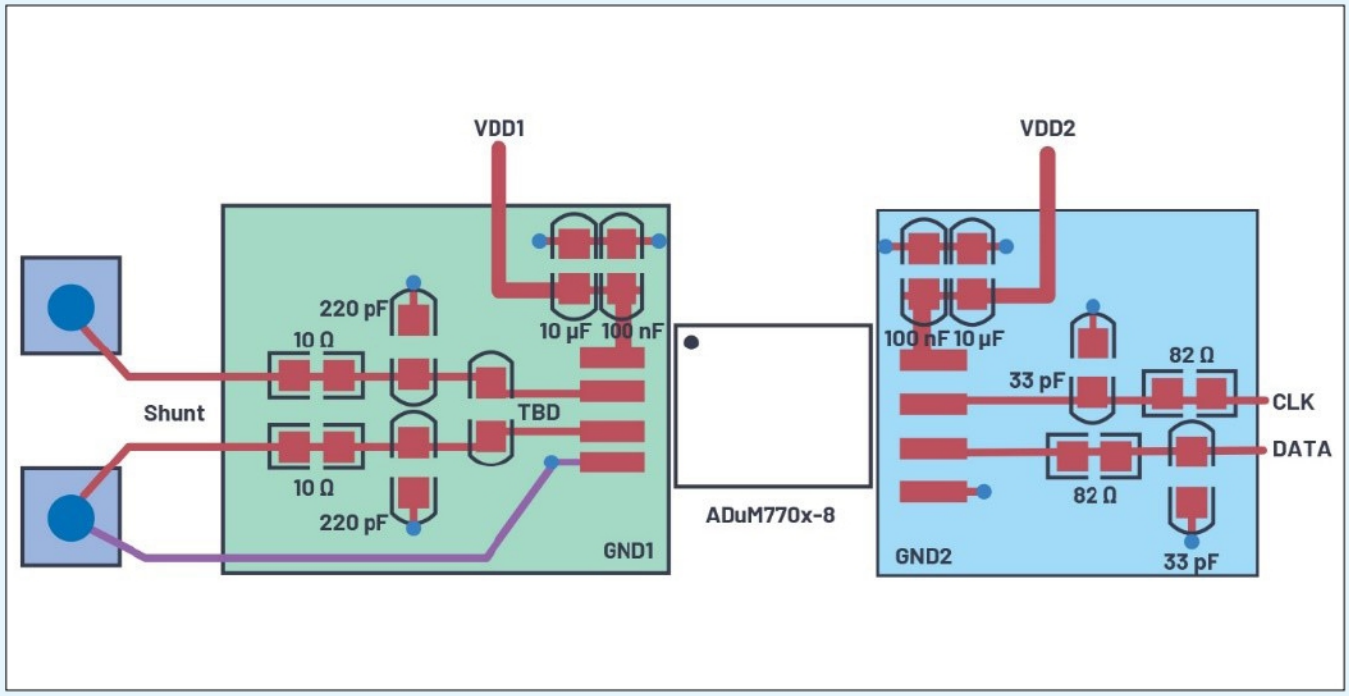


Figura 7: Layout del PCB raccomandato per un circuito con ADuM770x-8

notevolmente il progetto del sistema e riduce i tempi di calibrazione. Gli ultimi dispositivi ADuM770x presentano il più alto livello di isolamento e le migliori prestazioni del convertitore ADC.

È disponibile anche una versione con LDO, che può semplificare la progettazione dell'alimentazione del sistema (**Tabella 1**).

CIRCUITO E LAYOUT RACCOMANDATI

Nella **Figura 6** viene mostrato il tipico circuito di misura di corrente di un sistema di controllo motore. Sebbene questo sistema richieda tre circuiti di misura della corrente, uno per ogni fase, nello schema a blocchi ne viene illustrato solo uno. Gli altri due circuiti sono identici e sono indicati dalle linee tratteggiate blu. Dal circuito di misura

della corrente di fase si può notare che un lato del resistore R_{SHUNT} è collegato all'ingresso dell'ADuM770x-8. L'altro lato è collegato ai FET ad alta tensione (che possono essere IGBT o MOSFET) e al motore. Quando i FET ad alta tensione cambiano stato si verificano sempre condizioni di sovratensione, sottotensione o altre situazioni di instabilità elettrica. Di conseguenza, la fluttuazione di tensione del resistore R_{SHUNT} passerà all'ADuM770x-8 e i relativi dati verranno ricevuti sul pin DATA. La progettazione del layout e dell'isolamento del sistema può migliorare o peggiorare le condizioni di instabilità di tensione, che influiscono sulla precisione della misura della corrente di fase. L'implementazione circuitale consigliata, come illustrato nella **Figura 6**, prevede quanto segue:

- Per disaccoppiare VDD1/VDD2, sono necessari condensatori da 10 µF/100 nF che devono essere collocati il più possibile in prossimità dei pin corrispondenti.
- È necessario un filtro RC da 10 Ω/220 pF.
- Per ridurre gli effetti del rumore proveniente dallo shunt si raccomanda l'utilizzo di un condensatore opzionale, da collocare sulla linea differenziale in prossimità dei pin IN+/IN– (si consiglia di scegliere il package 0603).
- Quando la pista digitale d'uscita è lunga, si raccomanda di installare un filtro RC da 82 Ω/33
- Per ottenere buone prestazioni, si dovrebbe utilizzare un doppino intrecciato e schermato.
- Per i requisiti di prestazioni più elevate, si può valutare l'utilizzo di un resistore di shunt a 4-terminali.

Per ottenere le prestazioni migliori, è necessario anche un buon layout. Quello consigliato è illustrato nella **Figura 7**. Per migliorare la capacità di reiezione di modo comune, si consiglia di collegare la coppia differenziale dalla resistenza shunt ai pin di ingresso IN+/IN-.
Il filtro da 10 Ω/220 pF deve essere posizionato il più vicino possibile ai pin di ingresso IN+/IN-. I condensatori di disaccoppiamento da 10 µF/100 nF devono essere posizionati vicino ai pin di alimentazione VDD1/VDD2. Per migliorare la stabilità del segnale si raccomanda di implementare il piano di massa GND1 sotto il relativo circuito di ingresso.
La pista GND1 indipendente (indicata in viola e parallela alla linea di collegamento della coppia differenziale), deve essere collegata a stella dalla resistenza shunt al pin GND dell'ADuM770x-8, per ridurre l'effetto di fluttuazione della corrente di alimentazione.

CONCLUSIONE

I più recenti modulatori sigma-delta isolati ADuM770x aumentano il CMTI fino al livello di 150 kV/µs e migliorano le prestazioni di deriva in temperatura, fornendo grandi vantaggi alle applicazioni di misura della corrente. L'utilizzo del circuito e del layout consigliati potrà risultare utile in fase di progettazione.

RIFERIMENTI

Data sheet ADuM7704 . Analog Devices, Inc., Agosto 2020.

Heo, Hong-Jun; Seon-Ik Hwang; Jang-Mok Kim e Jin-Woo Choi. "Compensating of Common Scaling Current-Measurement Error for Permanent Magnet Synchronous Motor Drives." 2016 IEEE 8° Conferenza Internazionale "Power Electronics and Motion Control" (IPEMC-ECCE Asia), Maggio 2016.

Mary McCarthy: "AN-1131: Chopping on the AD7190, AD7192, AD7193, AD7194, and AD7195." Analog Devices, Inc., Ottobre 2011.

Miguel Usach Merino e Gerard Mora Puchalt: "Integrated Capacitive PGAs in ADCs: Redefining Performance." *Analog Dialogue*, Vol. 50, No. 3, Agosto 2016.

Nicola O'Byrne: "MS-2652: Measurement Techniques for Industrial Motion Control." Analog Devices, Inc., Giugno 2014.

Si ringrazia, per la collaborazione con Elettronica Open Source, Nandin Xu, Product Applications Engineer, Analog Devices.

L'autore è a disposizione nei commenti per eventuali approfondimenti sul tema dell'Articolo. Di seguito il link per accedere direttamente all'articolo sul Blog e partecipare alla discussione:
https://it.emcelettronica.com/come-migliorare-le-misure-di-corrente-a-livello-di-sistema-con-i-modulatori-isolati-sigma-delta-di-prossima-generazione

PROTEZIONE DELLE RETI IOT

di **Roberta Fiorucci**

Consentire ai dispositivi di connettersi a Internet li espone a una serie di gravi vulnerabilità se non sono adeguatamente protetti. La sicurezza IoT comprende tecniche, strategie e protocolli. In questo articolo parleremo di come l'IoT sia un punto debole per i cybercriminali, quali sono le vulnerabilità e gli errori e come la blockchain può essere considerata una contromisura.

INTRODUZIONE

Lo scambio continuo di dati che avviene attraverso gli oggetti connessi rappresenta un vantaggio tecnologico ma anche un problema di sicurezza e di privacy. Nei prossimi decenni la crescita dell'Internet of Things (**IoT**) sarà esponenziale e aumenteranno ulteriormente i rischi connessi.

A questo va aggiunto un ulteriore aspetto affatto trascurabile. L'IoT non è una tecnologia singola ma è la convergenza di più tecnologie che pur essendo eterogenee appartengono ad ambiti ingegneristici differenti.

Tecnologie che includono l'identificazione a radiofrequenza (**RFID**), il networking e la comunicazione, le reti di sensori wireless (WSN), i sistemi in tempo reale (RTS) ma anche edge e **cloud computing**, ad esempio. Tutto questo amplifica gli sforzi per rendere i sistemi più sicuri e al riparo da attacchi.

Solo nell'ultimo anno sono stati segnalati oltre 1,5 miliardi di attacchi informatici ai dispositivi IoT e se si considera che solo per il prossimo anno, il numero di dispositivi connessi alle reti sarà tre volte superiore alla popolazione mondiale, la sicurezza va vista come un aspetto centrale.

In questo articolo parleremo di come l'IoT sia un punto debole per i cybercriminali, quali sono le vulnerabilità e gli errori e come la blockchain può essere considerata una contromisura.

COSA È ACCADUTO NEGLI ANNI

La prima forma importante di un attacco IoT viene legata al virus Stuxnet. La particolarità di questo virus molto sofisticato è la sua capacità di danneggiare direttamente le strutture fisiche tramite dei drive USB infetti. Il primo bersaglio del virus (qualcuno suppone sia stato creato dagli americani in accordo con lo stato di Israele) è stato l'impianto iraniano di Natazan. Una struttura per il nucleare di 100mila metri quadrati costruita otto metri sotto terra di cui si è parlato anche di recente dopo un tentativo di attacco cyber alle reti elettriche. Nel 2010 subì un attacco, orchestrato e partito l'anno prima nonostante l'impianto nucleare fosse stato completamente air gap (niente internet, niente cavi di rete).

Il virus doveva disabilitare gli apparecchi centrifughi impedendo la rilevazione dei malfunzionamenti e, naturalmente, nascondendo la stessa presenza del virus.

Stuxnet ha preso così di mira il controllo di supervisione e i sistemi di acquisizione dati (SCADA) nel sistema di controllo industriale (ICS), utilizzando malware per infettare le istruzioni inviate dai controllori logici programmabili (**PLC**).

L'infezione viene fatta risalire ad alcuni fornitori iraniani che producevano componenti che erano a loro volta parte dei macchinari della centrale. Nel 2013 è stata scoperta da un ricercatore la prima botnet IoT costituita per oltre il 25% da dispositivi diversi dai computer, tra cui oltre a smart TV ed elettrodomestici comparivano anche i baby monitor.

Ma la rete più grande di dispositivi infettati legati all'IoT si chiama Mirai, che ha prodotto attacchi che hanno raggiunto chiunque e che si sono infiltrati nella rete attraverso dispositivi IoT di consumo come telecamere IP e router.

Mirai si autopropaga.

Il codice sorgente è stato reso pubblico da chi l'ha creato e ha prodotto numerose varianti. Il codice della botnet Mirai infetta i dispositivi poco protetti utilizzando il protocollo di rete telnet per trovare quelli che stanno ancora utilizzando il nome utente e la password predefiniti di fabbrica.

L'efficacia di Mirai è dovuta alla sua capacità di infettare decine di migliaia di questi dispositivi insicuri e di coordinarli per sferrare un attacco DDOS contro chiunque.

In sostanza, una volta parte della botnet, l'hardware dirottato viene cooptato per commettere altri attacchi.

Utilizzato per campagne di phishing e di spam, colpisce

in modo particolare siti Web o server. Infatti, lo sviluppo iniziale era diretto contro i server di gioco Minecraft ad opera di due studenti indiani (Paras Jha e Josiah White) che hanno fatto trapelare il codice online nel tentativo di oscurare le origini dei loro attacchi botnet.
Gli esempi di violazioni in tutto il mondo sono tantissimi. Una società di telecamere di sicurezza ha visto hackerare 150.000 feed delle telecamere live da un gruppo di hacker svizzeri.
Queste telecamere hanno monitorato l'attività all'interno di scuole, carceri, ospedali e strutture di aziende private, tra cui Tesla.
L'azienda di dispositivi medici St. Jude Medical ha creato dispositivi cardiaci i cui sistemi incorporati si sono dimostrati vulnerabili e molto pericolosi. Settori come quello automobilistico e sanitario hanno ampliato la loro selezione di sensori e dispositivi IoT.
Questo ha anche portato a rischi maggiori soprattutto perché la sicurezza è stata spesso trascurata a fronte di una produzione poco attenta alle diverse fasi di progettazione o votata a creare soluzioni il più possibile economiche.
Il primo grande errore legato alla sicurezza dei dispositivi parte proprio dalla loro nascita.

ECOSISTEMA IOT

La gestione e la creazione delle **soluzioni IoT** coinvolge più ambiti e persone: sviluppatori del software che eseguono i dispositivi IoT e ingegneri dell'hardware, che oltre ai dispositivi hardware creano anche processori e microcontrollori.
Analisti di dati che elaborano i dati dai dispositivi IoT e li trasformano in informazioni utili e fruibili. I responsabili della manutenzione dell'infrastruttura IoT, inclusa la gestione degli endpoint e del traffico di rete IoT durante tutto il ciclo di vita del dispositivo.

GLI STANDARD DI SICUREZZA LEGATI ALL'IOT

Esistono molti framework di sicurezza IoT ma ad oggi non esiste un unico standard universalmente riconosciuto. I framework di sicurezza IoT forniscono strumenti ed elenchi di controllo e in questo senso vanno a supportare la creazione e anche la distribuzione dei tanti dispositivi IoT. Sebbene non sia specifico per l'IoT, il Regolamento Generale sulla Protezione dei Dati (GDPR), pubblicato a maggio 2016, unifica le leggi sulla privacy dei dati in tutta l'Unione Europea.
Queste protezioni si estendono ai dispositivi IoT e alle loro reti e i produttori di dispositivi IoT dovrebbero tenerne conto. Nel mese di giugno 2022 è uscita la prima versione della ISO/IEC 27400:2022 “Linee Guida per la sicurezza e privacy dei dispositivi IoT”.
Si tratta di una linea guida, lungamente attesa, che va ad integrare la ISO/IEC 27000 sulla sicurezza delle informazioni. Il primo standard applicabile a livello globale per la sicurezza IoT dei consumatori è stato rilasciato nel 2019 dall'European Telecommunications Standards.
Gli Stati Uniti hanno introdotto l'Internet of Things Cybersecurity Improvement Act nel 2020, ordinando al National Institute of Standards and Technology di creare standard minimi di sicurezza informatica per quegli IoT controllati o di proprietà del governo degli Stati Uniti.

ERRORI BY DESIGN PIÙ FREQUENTI

La sicurezza informatica nei dispositivi deve partire fin dalla fase di progettazione. La protezione dei dispositivi non dovrebbe mai essere aggiunta in un secondo momento o in seguito ad una criticità. L'obiettivo di uno sviluppatore di soluzioni dovrebbe essere lo sviluppo di software sicuro e l'integrazione sicura.
Per coloro che implementano sistemi IoT, la sicurezza e l'autenticazione hardware sono misure critiche.

CORSO DI ELETTRONICA PER RAGAZZI – PUNTATA 3

di **Fulvio De Santis**

Nel precedente articolo "Corso di Elettronica per ragazzi - Puntata 2" abbiamo parlato dell'elettricità di movimento nei solidi e nei liquidi, ovvero della CORRENTE ELETTRONICA e della CORRENTE IONICA. In questo articolo parleremo ancora un pò della corrente elettrica e introdurremo il concetto di TENSIONE ELETTRICA, POTENZIALE ELETTRICO, DIFFERENZA DI POTENZIALE e vedremo cos'è e come funziona il GENERATORE ELETTRICO.

INTRODUZIONE

Nella **seconda parte del corso di Elettronica** abbiamo compreso cos'è la corrente elettrica, ossia il movimento di elettroni in una certa direzione, e abbiamo chiarito le definizioni di verso convenzionale e verso effettivo della corrente. Ma occorre capire un'altra cosa molto importante della corrente, specialmente quando cominceremo a realizzare circuiti elettrici: **COME SI MISURA LA CORRENTE** che scorre in un conduttore! Oppure, possiamo anche chiederci: "quanta elettricità passa attraverso un conduttore?". Per rispondere a questa domanda ci serviremo dell'immagine riportata in **Figura 1** in cui viene mostrato un conduttore attraverso il quale immaginiamo che scorra una corrente elettrica formata da elettroni in movimento verso una certa direzione.

Bene, la misura della corrente che scorre in questo **conduttore** si determina dalla quantità di elettroni che attraversano una SEZIONE del conduttore nell'intervallo di tempo di un secondo. Una SEZIONE è una superficie piana perpendicolare alla direzione della corrente, come quelle colorate in azzurro all'interno del conduttore mostrato in **Figura 1**. Questa quantità di elettricità che attraversa in un secondo una sezione del conduttore si chiama **INTENSITA'** di corrente. L'unità di misura dell'INTENSITA' di corrente è l'**AMPERE** (si pronuncia Amper) il cui simbolo è la lettera **A**. Vedremo che nelle formule e nella descrizione teorica dei circuiti, la corrente viene indicata con la lettera **I** o **i**.

Equivalente all'Ampere, la quantità di carica elettrica in movimento in un conduttore è rappresentata dal **COULOMB** (si pronuncia CULOMB) che è appunto l'unità di misura della quantità di carica elettrica. Il simbolo

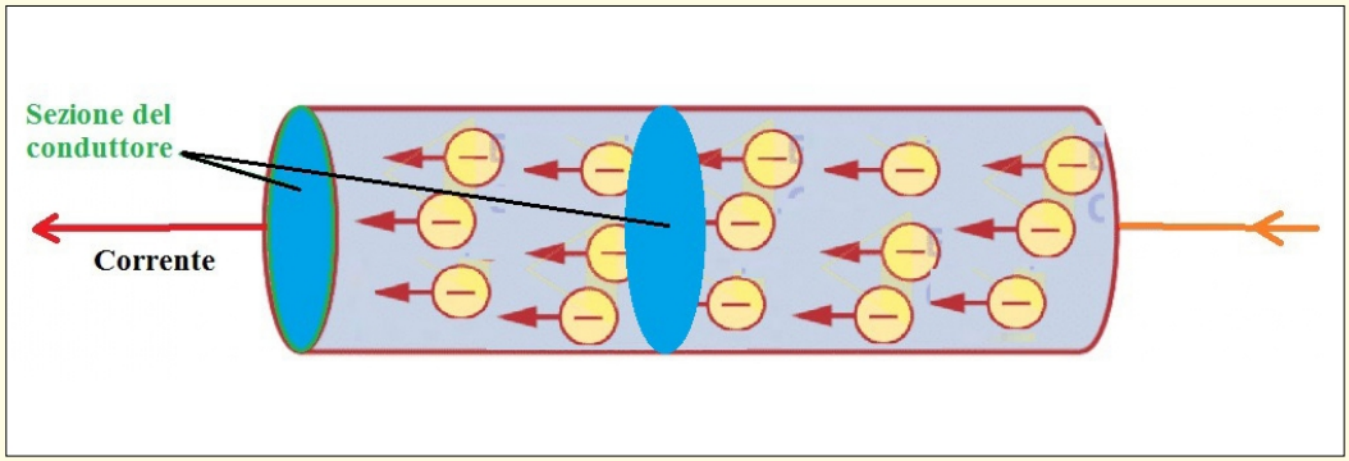


Figura 1: Corrente di elettroni che attraversa un conduttore

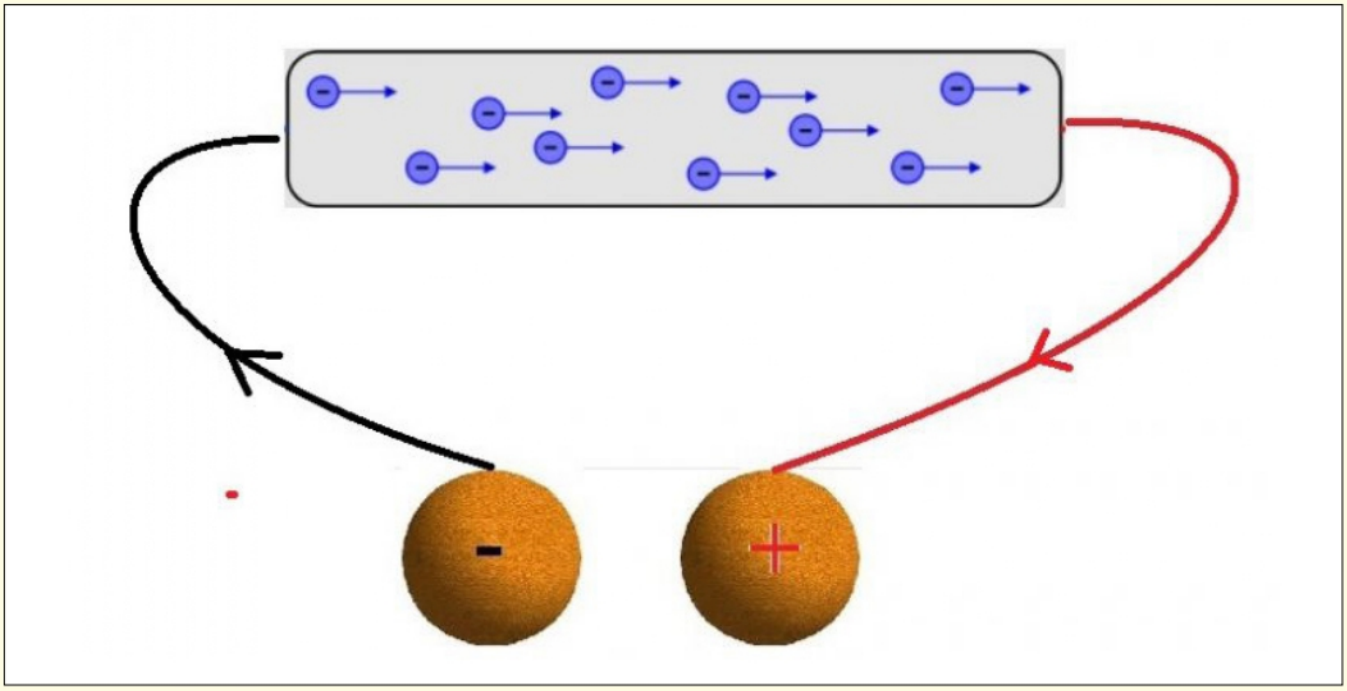


Figura 2: Cariche elettriche applicate ad un conduttore

del Coulomb è la lettera **C**, ma è possibile anche usare la lettera **Q**. Detto ciò, possiamo affermare che l'intensità di corrente è uguale al numero di coulomb al secondo che attraversano la sezione di un conduttore, ovvero, **un Ampere equivale ad un Coulomb al secondo**, in formula si scrive: **1 A = 1 C/s** .
Come vedremo, in pratica si usa l'AMPERE per misurare la corrente, ma il COULOMB può tornare utile usarlo quando viene descritta la teoria di funzionamento di alcuni componenti elettronici e fenomeni fisici.

POTENZIALE ELETTRICO E DIFFERENZA DI POTENZIALE

Consideriamo il funzionamento del sistema elettrico di

ve. In pratica, la creazione della corrente è stata possibile grazie alla differenza di cariche elettriche delle due sfere. In effetti, la sfera negativa possiede un **POTENZIALE** elettrico negativo superiore a quello della sfera positiva, e proprio questa **DIFFERENZA DI POTENZIALE** ha generato la corrente. Ciò è confermato dal fatto che non appena il sistema raggiunge l'equilibrio elettrico, ovvero le due sfere hanno la stessa carica elettrica, quindi lo stesso potenziale elettrico, il passaggio di corrente nel conduttore termina. La **DIFFERENZA DI POTENZIALE** è la **TENSIONE** esistente fra la sfera negativa e la sfera positiva. La TENSIONE viene indicata con la lettera **V** o **v**, e l'unità di misura è il **VOLT**. Come la corrente, anche la TENSIONE ha un verso detto **POLARITA'** indicata con + e -.

+ 140.000
REGISTERED USERS

7.414 AVERAGE DAILY PAGEVIEWS (FEB2020)

830.610 2020 ANNUAL VISITORS

THE BIGGEST **EMBEDDED COMMUNITY** IN ITALY

SOCIAL CONNECTIONS

+ 83.000

+ 23.000

CATEGORIES

COMPANIES/CONSULTANTS
53 %

ACADEMICS/STUDENTS
25 %

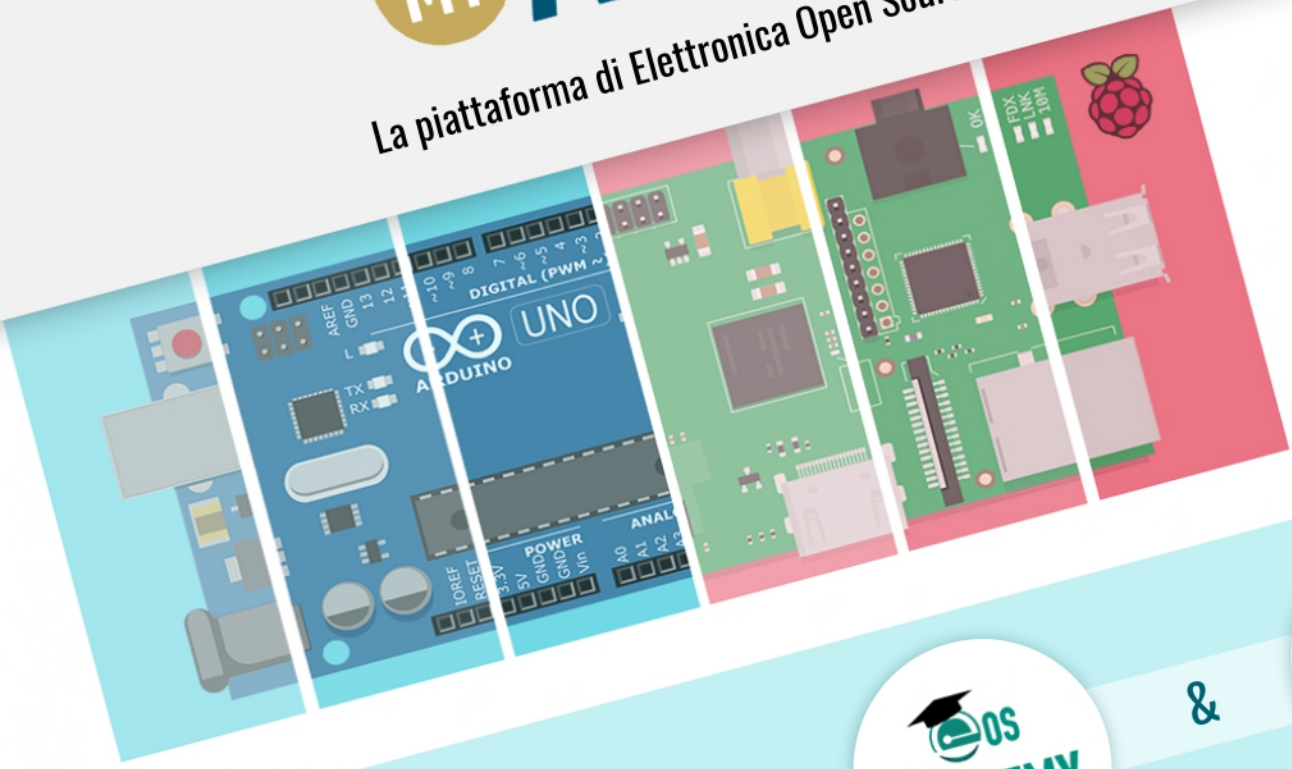
MAKERS/HOBBYISTS
22 %

Elettronica Open Source

I NOSTRI CORSI DI ELETTRONICA
PER I PROFESSIONISTI
E I MAKERS

MY ACADEMY

La piattaforma di Elettronica Open Source dedicata ai corsi



PUOI AVERE TUTTI I CORSI DI

EOS ACADEMY & MAKERS ACADEMY

A PORTATA DI CLICK