NUMERO 1 IN ITALIA SU ELETTRONICA EMBEDDED E SEMICONDUTTORI

Firmware 2.0

#60
Gen-Feb 2026

IoT Cybersecurity

IN QUESTO NUMERO:

COME SARÀ IL 2026 DELLA CYBERSECURITY?
CYBERSECURITY PER MAKERS: MINACCE REALI NEI PROGETTI CONNESSI
CORSO DI ELETTRONICA APPLICATA: GLI ALIMENTATORI SWITCHING - PARTE 1

E MOLTI ALTRI ARTICOLI E PROGETTI!

it.emcelettronica.com

Elettronica Open Source

PROFESSIONAL & MAKER ZONE

Versatili MCU Arm® Cortex®-M0+

Offrono Efficienza, Affidabilità e Innovazione Touch

Scoprite nuove possibilità nelle applicazioni IoT, consumer, industriali e automobilistiche con le famiglie di microcontroller PIC32CM GV00 e PIC32CM JH00. Basati sull'efficiente core Arm® Cortex®-M0+ con prestazioni fino a 48 MHz, questi MCU offrono un equilibrio ideale tra prestazioni, funzionamento a bassissimo consumo energetico e integrazione avanzata, su misura per soddisfare le esigenze del mondo connesso di oggi.

Il microcontroller PIC32CM16/32 GV00 è progettato per dispositivi ricchi di sensori e attenti al consumo energetico, combinando un funzionamento a bassissimo consumo (da soli 1,62 V a 3,63 V) con caratteristiche leader di mercato come un controller touch capacitivo a 256 canali, analogico di precisione e connettività flessibile. Questo lo rende una scelta eccellente per i prodotti IoT e di consumo in cui la reattività e l'efficienza sono fondamentali.

Per gli ambienti in cui affidabilità e stabilità sono fondamentali, l'MCU PIC32CM32/64 JH00 si distingue per il robusto funzionamento a 5 V, la forte integrazione analogica e la tecnologia touch avanzata Driven Shield+. Ciò garantisce prestazioni touch capacitive affidabili, anche in presenza di superfici bagnate o in condizioni di elevata interferenza, rendendolo la scelta affidabile per controlli industriali, sistemi automobilistici ed elettrodomestici avanzati.

Che tu stia sviluppando dispositivi compatti e sensibili ai costi o applicazioni impegnative in ambienti difficili, le famiglie di MCU PIC32CM GV00 e PIC32CM JH00 offrono le caratteristiche, l'affidabilità e le prestazioni necessarie per competere e avere successo.

MICROCHIP
PIC32CM32/64 JH00

MICROCHIP
PIC32CM16/32 GV00

MICROCHIP

microchip.com/pic32cm-gv-jh

MEC2634A-ITA-12-25

Firmware 2.0 EDITORIAL PLAN 2026

COSA LEGGERAI NEL 2026?

TOPICS	MAKERS ZONE	DATA DI PUBBLICAZIONE
IoT	Cybersecurity	1 Febbraio
Artificial Intelligence	Edge Machine Learning	1 Marzo
Power/Motor	Green Energy	1 Aprile
PCB	Microcontrollers	1 Maggio
Test & Measurements	DIY Tools	1 Giugno
Automotive	Sensors	1 Luglio
Open-Source	Development Boards	1 Settembre
Wireless/RF	LoRa Networks	1 Ottobre
Industry 4.0	Automation & Robotics	1 Novembre
Healthcare	Medical Wearable	1 Dicembre

IoT e Cybersecurity al centro dell'elettronica connessa

Cari lettori,

con il numero 60 di Firmware 2.0 apriamo il nuovo anno editoriale e inauguriamo una nuova fase della nostra rivista. Un traguardo importante che coincide con un tema quanto mai attuale e strategico, il ***binomio IoT/Cybersecurity****, due mondi ormai inseparabili che definiscono il presente e, soprattutto, il futuro dell'elettronica applicata. Da promessa tecnologica, l'Internet of Things è diventata una realtà diffusa, il cui principale merito è aver trasformato l'elettronica in un ecosistema aperto, distribuito e interconnesso. Sensori, microcontrollori e sistemi embedded popolano le nostre case, le fabbriche, le città, e persino i dispositivi che indossiamo. Progettare, oggi, significa* ***pensare in termini di reti, protocolli di comunicazione, cloud, edge computing e gestione intelligente*** *dei dati, una nuova visione che ha abbassato le barriere di accesso aumentando però in modo esponenziale la complessità dei sistemi. Qui entra in gioco la Cybersecurity.* ***Ogni dispositivo connesso è un potenziale punto di accesso, ogni firmware una possibile superficie di attacco****, per questo la sicurezza non può più essere considerata un'aggiunta tardiva o un optional, ma deve essere* ***parte integrante del progetto elettronico*** *a partire dalle prime fasi di design. Crittografia, autenticazione, secure boot, aggiornamenti OTA sicuri e gestione delle vulnerabilità, precedentemente concetti riservati agli specialisti IT, sono diventate competenze fondamentali anche per chi lavora con schemi elettrici, PCB e codice embedded. In questo numero esploriamo l'IoT e la Cybersecurity con un approccio pratico e divulgativo, fedele allo spirito di Firmware 2.0, analizzando tecnologie, architetture e casi d'uso reali, sia per fornire strumenti di comprensione e chiavi di lettura utili a progettisti, studenti e appassionati, sia per facilitare la comprensione del funzionamento di tutto ciò che progettiamo, e il modo in cui proteggerlo. Il numero 60 segna anche un passaggio importante nella nostra proposta editoriale. Prende il via il nuovo* ***Corso di Elettronica Applicata****, una serie a puntate pensata per accompagnare il lettore dalla teoria alla pratica, dal singolo componente al sistema completo. Il corso raccoglie il testimone del precedente "Corso di Elettronica per ragazzi" concluso con il numero di dicembre, ampliandone l'orizzonte e alzando progressivamente il livello di approfondimento. Il percorso è pensato per chi vuole consolidare le basi dell'elettronica reale che dialoga con il mondo fisico e digitale. In un'epoca di oggetti intelligenti e reti globali, l'elettronica è chiamata ad essere innovativa e responsabile, ed è con questo spirito che vogliamo contribuire a formare progettisti consapevoli, capaci di costruire sistemi connessi che siano anche robusti e sicuri.*

Buona lettura e buon 2026 con Firmware 2.0!

Giordana Francesca Brescia

Anticipa la tempesta

Il tuo riparo dalle intemperie dell'inventario

mouser.it/customer-resource-center

MOUSER ELECTRONICS

IoT Cybersecurity

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 - 149.241
Social Network - 130.492

EDITORIALE
IOT E CYBERSECURITY AL CENTRO DELL'ELETTRONICA CONNESSA 3

I PRINCIPALI TREND 2026-2030 SULL'IOT SECURITY 7

LE NOVITÀ DEL 2026 NEL SETTORE DELL'ELETTRONICA 8

CRITTOGRAFIA E VULNERABILITÀ NELL'ERA QUANTISTICA 11

IBM ACCELERA SUL QUANTUM COMPUTING E SFIDA GOOGLE CON ARCHITETTURE INNOVATIVE PER SUPERARE I LIMITI DEI QUBIT 15

COME SARÀ IL 2026 DELLA CYBERSECURITY? 17

CYBERSECURITY PER LE RETI DI AUTOMAZIONE INDUSTRIALE 18

CYBERSECURITY EMBEDDED NEI DISPOSITIVI IOT 22

CYBERSECURITY PER MAKERS: MINACCE REALI NEI PROGETTI CONNESSI 24

PENETRATION TEST PER DISPOSITIVI EMBEDDED 28

SICUREZZA NELLA SMART HOME – COME PROTEGGERE IL NOSTRO ECOSISTEMA IOT DOMESTICO 30

DECORIAMO UN ALBERO DI NATALE CON LUCI E RIPRODUZIONE DI MUSICHE UTILIZZANDO ARDUINO 32

I SENSORI INVISIBILI CHE CI CIRCONDANO: 10 ESEMPI NELLA VITA QUOTIDIANA 38

CORSO DI ELETTRONICA APPLICATA: GLI ALIMENTATORI SWITCHING – PARTE 1 40

CES 2026 SENZA GPU NVIDIA – IL SEGNALE DI UNA CRISI PROFONDA NEL MERCATO DEI PC? 46

DOVE FINISCE IL 70% DELLA PRODUZIONE GLOBALE DI RAM? 47

ARDUINO UNO Q 4GB, IL SINGLE BOARD COMPUTER CHE PORTA ARDUINO NELL'ERA LINUX 48

ESP32-E22: IL NUOVO CO-PROCESSORE WI-FI 6E DI ESPRESSIF PER LA CONNETTIVITÀ WIRELESS AVANZATA 49

COME SARÀ IL 2026 DELLA CYBERSECURITY?

di **Redazione**

Nel 2026 la sicurezza digitale sarà caratterizzata da AI autonome, cloud frammentati e nuove vulnerabilità. Scopriamo in questo articolo trend e prospettive del settore.

La **cybersecurity** si prepara ad affrontare un cambiamento strutturale che va ben oltre l'aggiornamento degli strumenti tecnologici, imponendo alle imprese un profondo cambio di approccio. L'anno appena concluso ha accelerato dinamiche già in atto, rendendo evidente come l'evoluzione dell'Intelligenza Artificiale, unitamente alla crescente stratificazione degli ambienti cloud e all'ibridazione delle minacce, stiano modificando le priorità della difesa digitale. In questo contesto, la sicurezza non potrà più essere considerata un dominio esclusivamente tecnico, bensì un sistema complesso in cui tecnologia, governance e comportamento umano risultano indissolubilmente legati.

L'adozione diffusa di **modelli generativi** e di **agenti AI** sempre più autonomi sta modificando il perimetro stesso del rischio, con le superfici di attacco che non coincidono più soltanto con reti, endpoint o applicazioni, ma si estendono ai processi che alimentano l'intelligenza delle macchine; nel mentre, i flussi di dati utilizzati per addestrare i modelli diventano un obiettivo strategico, poiché anche un'alterazione minima e difficilmente rilevabile può produrre effetti sulle decisioni automatiche a valle. La **sicurezza dei dati**, in questa prospettiva, si trasforma in **sicurezza delle pipeline**, imponendo controlli continui sull'origine, sull'integrità e sull'affidabilità delle informazioni utilizzate dai sistemi di AI. Parallelamente, gli assistenti intelligenti stanno guadagnando terreno nelle operazioni aziendali, in cui da semplici strumenti di supporto, si stanno evolvendo in veri e propri attori digitali

sistema autonomo richiede una valutazione di fiducia, una definizione precisa dei privilegi e un monitoraggio comportamentale continuo, al punto che anche le tecniche di ingegneria sociale si adattano a questo scenario, spostando l'attenzione dall'inganno dell'utente umano alla manipolazione dei flussi di istruzioni che guidano le **AI**. Si comprende facilmente che la sicurezza sta diventando una disciplina che deve comprendere e anticipare il modo in cui le macchine interpretano contesti, richieste o dati.

A complicare ulteriormente il quadro, contribuisce la proliferazione di modelli e infrastrutture non governate. In molte organizzazioni stanno emergendo ambienti paralleli in cui sviluppatori e team sperimentano soluzioni AI al di fuori dei controlli centrali, replicando dinamiche già viste con lo Shadow IT. Server locali, protocolli di contesto e modelli collegati a servizi pubblici rischiano così di ingerire dati sensibili senza alcuna tracciabilità né supervisione, con un aumento dell'esposizione complessiva. E' evidente, a questo punto della trattazione, che il fattore umano riacquista un ruolo decisivo. **La tecnologia rimane un moltiplicatore di capacità, ma non può sostituire il giudizio, la responsabilità e la visione sistemica**.

> *"Nel 2026, le organizzazioni più resilienti saranno quelle in grado di integrare governance rigorosa, consapevolezza diffusa e competenze trasversali.*

CYBERSECURITY PER MAKERS: MINACCE REALI NEI PROGETTI CONNESSI

di **Daniele Valanzuolo**

La sicurezza nei progetti maker non è più un optional. I dispositivi connessi, anche quelli autocostruiti o destinati all'uso hobbistico, sono oggi parte di reti reali, esposti a rischi concreti e, talvolta, sfruttati in modo inconsapevole per attività malevole. Chi progetta sistemi connessi, anche dalla propria cameretta o tra le pagine di un blog tecnico, ha una responsabilità implicita: quella di non contribuire, anche involontariamente, all'insicurezza globale della rete. Fortunatamente, oggi esistono strumenti open-source, librerie robuste, ambienti di sviluppo maturi e risorse accessibili per costruire dispositivi più sicuri senza costi aggiuntivi e con un minimo impatto sul ciclo di sviluppo. In questo articolo, andremo ad affrontare alcuni aspetti e concetti base di cybersecurity, osservando le buone pratiche di progettazione e una checklist base per rendere più sicuri i nostri progetti.

INTRODUZIONE

Negli ultimi anni, i progetti elettronici fai-da-te hanno fatto un salto enorme grazie all'evoluzione tecnologica e all'hardware low-cost disponibile sul mercato. Infatti, bastano pochi componenti, una scheda ESP32 e qualche riga di codice per realizzare sensori connessi, automazioni, dispositivi indossabili o centraline che comunicano, Bluetooth o Wi-Fi. Una rivoluzione silenziosa che ha avvicinato migliaia di makers al mondo dell'**Internet of Things**. Purtroppo, connesso non vuol dire sicuro, anzi la connettività incrementa notevolmente i rischi, e troppo spesso questi ultimi sono sottovalutati da chi realizza progetti. Dal punto di vista della cybersecurity, la questione non è se un dispositivo sia interessante per un attaccante.

> *"La realtà è che ogni oggetto connesso, anche il più banale, può diventare un punto d'ingresso per tutta la rete.*

Anche semplicemente un relè Wi-Fi installato in casa, se configurato in maniera errata, può finire esposto su Internet e concedere una porta di accesso aperta ai malintenzionati. Anche se consideriamo un'app per controllare le luci via Telegram, questa può rivelare token e API in chiaro. Una telecamera artigianale costruita con un Raspberry e un web-server improvvisato può trasformarsi in una finestra aperta sulla propria vita. **Succede ogni giorno**, spesso senza che chi ha realizzato il progetto se ne accorga.

Un altro fattore di enorme rischio è la frequenza con cui **molti makers pubblicano con entusiasmo il proprio codice su GitHub**, condividono schemi e firmware, ma dimenticano di rimuovere le credenziali, i certificati, le chiavi. Questo, spesso capita anche nei tutorial, nei forum e nei progetti open-source. Non c'è malizia, solo inesperienza nel valutare il rischio. Purtroppo, l'effetto è lo stesso: porte aperte disponibili per i malintenzionati, e quindi, quello che per noi è un passatempo creativo può diventare un problema serio.

Con questo articolo andremo ad analizzare le minacce concrete **nei progetti connessi fai-da-te**, partendo da casi realmente accaduti, errori comuni e cattive pratiche che circolano online.

> *"L'obiettivo è sensibilizzare e fornire consapevolezza a tutti i progettisti makers e professionisti.*

Fare bene le cose non vuol dire solo farle funzionare, ma anche proteggerle. Vedremo che, anche con pochi strumenti e un pò di attenzione in più, possiamo incrementare il livello di difesa dei nostri progetti.

ESEMPIO PRATICO

Passiamo ora ad un piccolo esempio pratico, semplice ma esplicativo. È bene tenere a mente che **negli ambienti reali gli attacchi non avvengono mai in modo isolato**. Una singola vulnerabilità raramente porta ad un

effetto critico immediato. Più spesso, ciò che si verifica è una catena di compromissione, cioè una sequenza di condizioni sfruttate in cascata. Questo concetto, già ben noto nella cybersecurity aziendale, vale anche nei progetti maker, dove spesso coesistono superficialità nella configurazione, componenti open-source scarsamente manutenuti e un'infrastruttura cloud poco sorvegliata. Dunque, immaginiamo un progetto con una scheda basata su ESP32 che raccoglie dati ambientali e li invia via MQTT ad un broker pubblico per visualizzazione tramite Home Assistant. Esistono tantissimi di questi progetti open-source e sempre più spesso il codice è stato condiviso su GitHub, completo del file config.h con token, password MQTT e credenziali Wi-Fi scritte in chiaro. Di conseguenza, chiunque cloni il repository ha accesso al broker, ai topic, e può pubblicare o ricevere messaggi. Inoltre, se il firmware supporta comandi remoti via MQTT, come reboot o reset dei sensori, l'attaccante ottiene anche un canale di controllo del dispositivo.
Da lì, la catena può estendersi:

- tramite le credenziali Wi-Fi, l'attaccante accede alla rete locale o ne deduce la configurazione;
- se Home Assistant è esposto via Internet con

sattivare allarmi a distanza, pubblicando pacchetti con mosquitto_pub. Nessuna autenticazione, nessuna cifratura. La catena può diventare anche fisica. Un beacon BLE installato per rilevare prossimità, può trasmettere in chiaro l'UUID. Spoofando quell'UUID, l'attaccante può fingere di essere il possessore del dispositivo, attivare scenari domotici o disattivare allarmi. In molti casi, i dispositivi non implementano autenticazione a livello BLE né whitelisting degli indirizzi MAC. Anche la componente cloud può essere l'anello debole. Alcuni progetti utilizzano servizi con API key visibili. Se l'account è configurato per inviare notifiche o aggiornare dati critici, il danno diventa potenziale: un attaccante può inviare messaggi ingannevoli all'utente, interferire con dashboard, raccogliere informazioni sensibili o addirittura modificare configurazioni.

BUONE PRATICHE DI SICUREZZA PER MAKERS

In tutti i casi elencati pocanzi, **il progetto originale funziona, ma non è protetto**, ed è proprio la fiducia nella sua correttezza a renderlo pericoloso; tuttavia, è possibile elevare il livello di sicurezza dei progetti maker.

CORSO DI ELETTRONICA APPLICATA: GLI ALIMENTATORI SWITCHING – PARTE 1

di **Fulvio De Santis**

Con questo articolo diamo ufficialmente inizio al Corso di Elettronica Applicata. Nelle diverse puntate ci sarà la descrizione di progetti più o meno complessi di vari dispositivi elettronici analogici e digitali, con l'obiettivo di consentire ai lettori di approfondire le basi della progettazione attraverso l'analisi dei circuiti. Inizieremo con gli alimentatori switching, che tratteremo in due puntate, una teorica e una progettuale. In questo articolo, nello specifico, presenteremo la parte teorica in cui andremo a descrivere il principio di funzionamento degli alimentatori switching step-down e step-up. Nella seconda parte che presenteremo nel prossimo articolo, faremo alcuni esempi di progetti mediante i quali vedremo come progettare gli alimentatori switching step-down e step-up utilizzando il circuito integrato MC34063A. Spiegheremo quali sono le differenze tra queste due tipologie di alimentatori e come si calcolano i componenti necessari alla loro realizzazione. Come vedremo, con l'impiego dell'integrato MC34063A, la progettazione di un alimentatore switching non presenta particolari difficoltà.

INTRODUZIONE

Rispetto al classico **alimentatore** stabilizzato di tipo lineare, progettare, realizzare e far funzionare un alimentatore di tipo switching è abbastanza complicato, anche se non è difficile comprenderne il principio dl funzionamento. Gli **alimentatori switching** hanno una **complessa conformazione circuitale**, oltre ad una maggiore attenzione da prestare in fase di realizzazione, in quanto occorre mettere in pratica alcuni accorgimenti costruttivi. A parte le difficoltà succitate, uno dei vantaggi è il fattore di forma: peso e dimensioni ridotti, infatti, rendono l'alimentatore switching un dispositivo molto compatto e leggero, quindi, la scelta ideale per alimentare apparecchiature elettroniche che devono occupare poco spazio. Grazie a queste caratteristiche, è possibile realizzare dispositivi sempre più miniaturizzati ed efficienti, come notebook, lettori DVD, caricabatterie per smartphone, e molti altri device.

Un'altra peculiarità degli alimentatori switching è di potere ottenere in uscita una tensione più alta di quella applicata in ingresso (alimentatore step-up), funzionalità impossibile da realizzare mediante il classico alimentatore stabilizzato lineare, che in genere utilizza un transistor di potenza come elemento di regolazione sul quale avviene la caduta di tensione che consente di regolare la tensione in uscita. In questo caso, il transistor lavora come una resistenza variabile posta in serie al carico. Ne consegue che la tensione di uscita è sempre inferiore a quella in ingresso. Tuttavia, seppur svolga perfettamente la sua funzione, questo sistema di regolazione ha lo svantaggio di un rendimento piuttosto basso, generalmente compreso tra 30% e 80%, dato che una parte non trascurabile della potenza fornita in ingresso viene dissipata in calore sull'elemento di regolazione (nel nostro esempio è un transistor) su cui deve essere montato un adeguato dissipatore di calore per evitarne il surriscaldamento durante il normale funzionamento.

Con l'alimentatore switching, non solo è possibile ottenere in uscita valori di tensione superiori a quelli di ingresso, ma soprattutto si raggiunge un rendimento dell'80-90%, molto più elevato del rendimento dell'alimentatore classico, che permette di ridurre notevolmente sia le sue dimensioni che quelle del dissipatore termico e del trasformatore di alimentazione; tutto ciò consente di prolungare i tempi di esercizio delle apparecchiature alimentate a batteria.

Oltre ai rilevanti vantaggi dell'alimentatore switching, presenta anche alcuni svantaggi, come un ripple sovrapposto alla tensione continua di uscita e la presenza di rumore ad alta frequenza, che rendono l'alimentatore switching sconsigliabile in alcune applicazioni sensibili ai disturbi e interferenze elettromagnetiche, mentre, ad esempio, per uso in laboratorio, oppure per gli amplificatori Hi-Fi, l'alimentatore tradizionale risulta più adatto. Per ovviare alla difficoltà di progettazione degli alimentatori switching, sono presenti da tempo sul mercato numerosi circuiti integrati, che consentono anche all'hob-

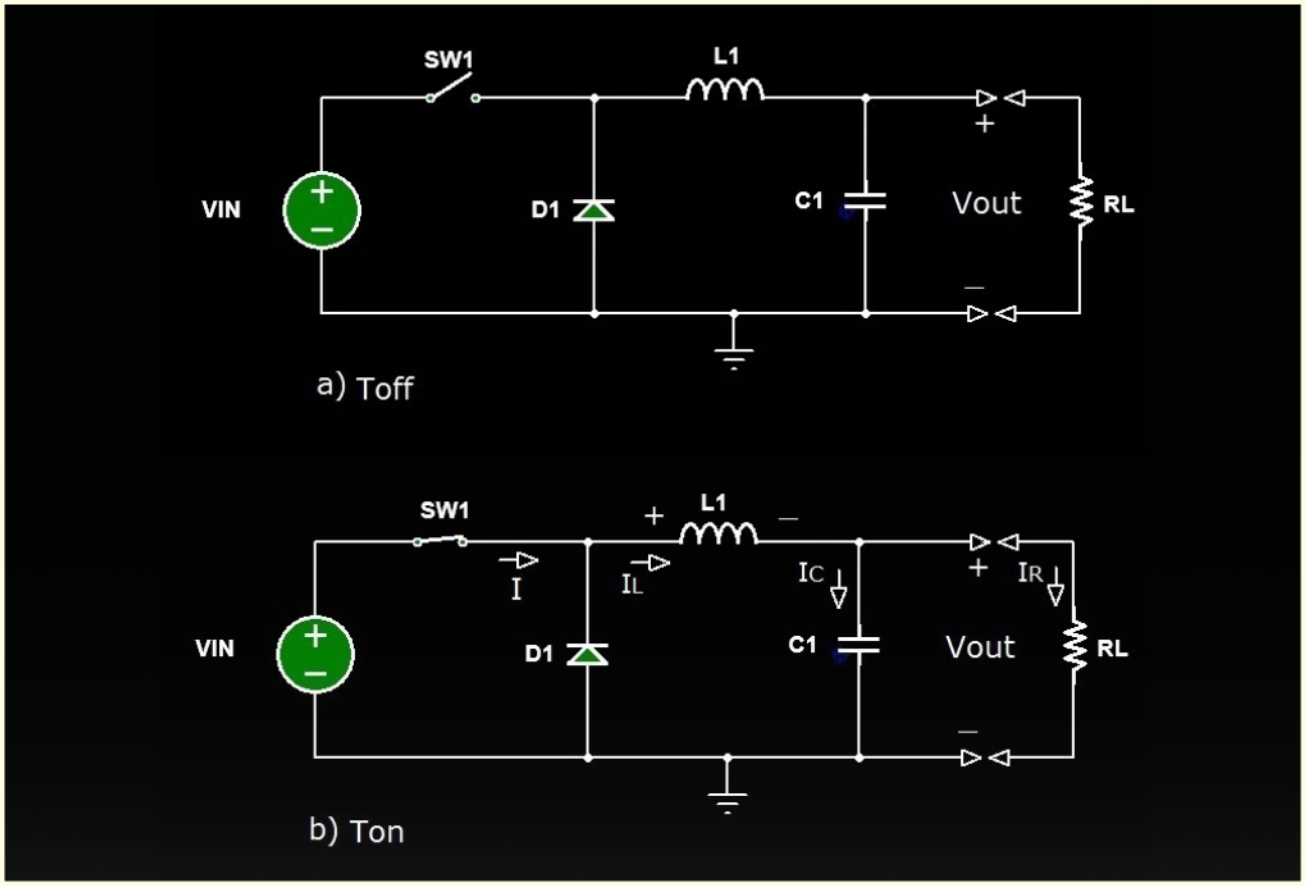

Figura 1: Schema di principio di un alimentatore switching step-down

bista di realizzare il tipo di alimentatore switching di cui ha necessità. Uno di questi è l'integrato MC34063A, che consente di realizzare una vasta tipologia di alimentatori switching sia step-down che step-up. In questo articolo, descriveremo il principio di funzionamento di due tipi principali di alimentatore switching: lo step-down, con il quale la tensione continua di uscita è di valore inferiore a quello della tensione applicata in ingresso; lo step-up, che permette di ricavare una tensione continua in uscita superiore a quella in ingresso.

nua, ipotizzando provenga da un circuito raddrizzatore e livellatore di tensione, oppure da una batteria, che nello schema è rappresentata dal generatore di tensione VIN. In serie alla linea di ingresso è posto un interruttore (SW1), a valle del quale si trova l'induttore L1 che risulta in serie al parallelo del condensatore C1 con il carico rappresentato dal resistore RL. Ad un terminale dell'induttore è collegato il catodo del diodo D1 il cui anodo è a massa. La tensione Vout ai capi di RL è la tensione di uscita dell'alimentatore.

L'ALIMENTATORE SWITCHING STEP-DOWN

Per comprendere come funziona l'alimentatore swi-

ABBONATI A

Firmware 2.0

PER AVERE **TUTTA L'ELETTRONICA A PORTATA DI CLICK** E RESTARE SEMPRE **AGGIORNATO SULL'ELETTRONICA EMBEDDED, I MICROCONTROLLORI** E **L'INNOVAZIONE TECNOLOGICA**

Elettronica Open Source

+ 150.000
REGISTERED USERS

+80.000 AVERAGE MONTHLY PAGEVIEWS

+500.000 2025 ANNUAL VISITORS

THE BIGGEST **EMBEDDED COMMUNITY** IN ITALY

SOCIAL CONNECTIONS

+ 85.000

+ 30.000

CATEGORIES

PROFESSIONALS
53 %

ACADEMICS/STUDENTS
25 %

MAKERS/HOBBYISTS
22 %

Elettronica Open Source