ANNO OTTO NUMERO DUE - BIMESTRALE - MARZO/APRILE 2024 - € 4,00

ÈUREKA!

INSIDE THE FUTURE

CRONACA DELL'INNOVAZIONE

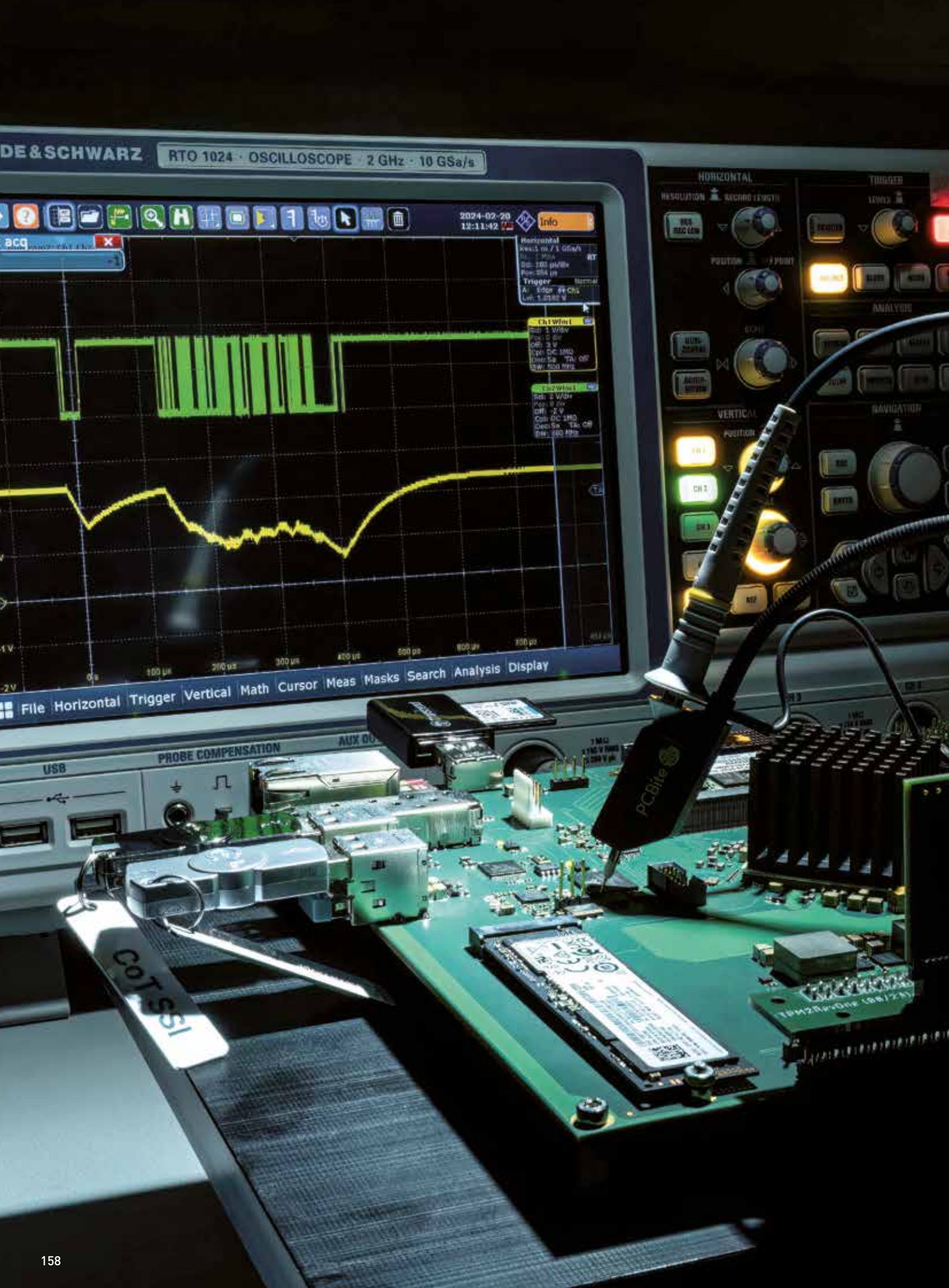
COVER STORY
Dagli SCARA ai collaborativi, i robot FANUC si prestano a realizzare ogni tipo di applicazione per il packaging e la pallettizzazione
p. 26

COLLECTION
La via di iMAGE S all'innovazione nei sistemi di visione contribuisce a generare occupazione ed effetti positivi per la comunità
p. 35

FOCUS ON PCB/JOURNAL
L'industria italiana dei circuiti stampati attende il rimbalzo nel 2024. E si dà appuntamento a Fiera di Vicenza il 15 e 16 maggio
p. 117

Poste Target Magazine LO/CONV/00388/02.2018 - P.I. 19/03/2024

ISSN 2704-808X

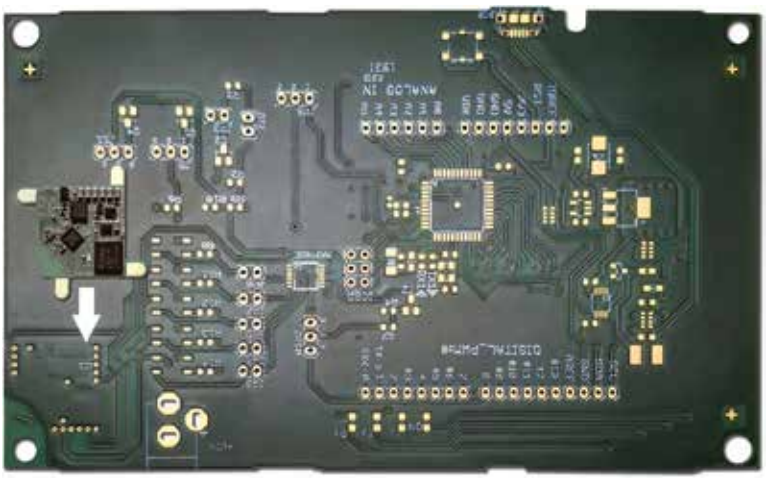

DE&SCHWARZ
RTO 1024 · OSCILLOSCOPE · 2 GHz · 10 GSa/s
HORIZONTAL
TRIGGER
VERTICAL
NAVIGATION
File Horizontal Trigger Vertical Math Cursor Meas Masks Search Analysis Display
PROBE COMPENSATION
USB
PCBite
CoTSSI

Identità digitali **affidabili**

Il progetto VE-ASCOT, coordinato da Wibu-Systems, è uno sforzo internazionale di ricerca e sviluppo che mira a creare un'identità digitale (DID) per i sistemi elettronici. Documenta il ciclo di vita di un componente, dalla produzione agli stadi di installazione, operatività e manutenzione, e garantisce l'integrità, autenticità e affidabilità del dispositivo hardware.

DI ALESSANDRO VELLA

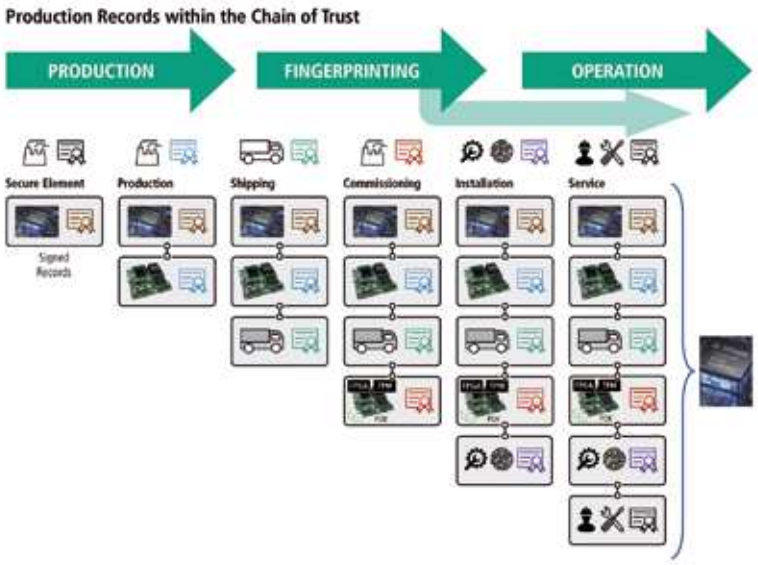
Le molte sfide intrinseche nella produzione di sistemi elettronici complessi sono state esacerbate da catene di approvvigionamento sotto stress e un numero crescente di scenari di minacce informatiche che influenzano l'affidabilità dei componenti elettronici e, di conseguenza, quella delle apparecchiature che li incorporano.
Il progetto di ricerca e sviluppo VE-ASCOT, coordinato da Wibu-Systems e che coinvolge Siemens, Infineon, Schölly Fiberoptic, Revisionone Engineering, l'Istituto Fraunhofer SIT e i laboratori di sicurezza Kastel, mira a creare un'identità digitale (DID) per i sistemi elettronici. Questa DID è una serie di record dati basata su blockchain che documenta il ciclo di vita di un componente elettronico in ordine cronologico. Questi record sicuri ed interconnessi, che vanno a creare la cosiddetta "Catena di Fiducia" (CoT), sono progettati per essere costantemente accessibili, verificabili ed espandibili.



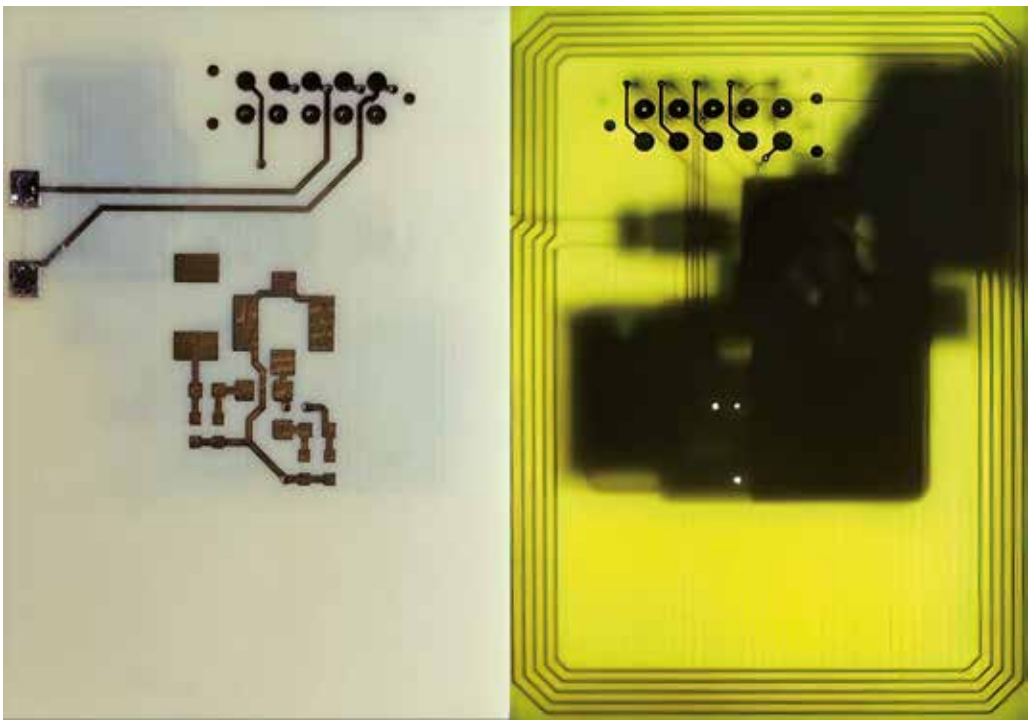
SE wireless con CoT laminato all'interno di un PCB.
Wireless SE with CoT laminated inside a PCB.

ANCORARE LA FIDUCIA: IL PRIMO ANELLO DELLA CATENA

La CoT inizia con una chiave segreta asimmetrica ed un certificato associato, la cui autenticità può essere verificata in qualsiasi momento.
La CoT viene memorizzata in un elemento sicuro (SE), protetto contro gli attacchi informatici. Con il suo numero di serie e i dati aggiuntivi, che vengono sottoposti a hash e firmati, questo certificato originale rappresenta il primo record dati nella CoT, rendendolo l'àncora di fiducia e un elemento del DID.
Tutti i passaggi successivi (produzione, messa in servizio, operatività e manutenzione del sistema), possono essere integrati nella CoT come record dati. Persino i dati doganali o di certificazione potrebbero farne parte, anche tramite valori hash crittografici che proteggono i riferimenti a record esterni. Ogni record dati della CoT è crittograficamente reso sicuro da una firma, utilizzando un'infrastruttura a chiave pubblica (PKI), che racchiude, ad esempio, certificati del produttore, della macchina o dell'operatore.
Nel tempo, la CoT nell'SE si arricchisce: ogni record crea un'identità sempre più dettagliata del sistema elettronico, che può essere validata in qualsiasi momento, consentendo una verifica locale e indipendente dell'affidabilità dei sistemi. Anche le risposte di feedback possono generare di per sé dei record.
Per meglio proteggere l'SE, questo può essere integrato nel PCB.
I PCB con uno spessore di 1,6 e 1,1 mm, equipaggiati con un'antenna NFC interna e che effettuano harvesting energetico per operare l'SE, permettono di leggere il DID preimpostato in modalità wireless.
Copie della CoT possono anche essere memorizzate su cloud, rendendo possibile, ad esempio, il controllo della distribuzione di aggiornamenti per interi impianti industriali da cloud o la mappatura di componenti e macchine in gemelli digitali.



Nella produzione distribuita di sistemi elettronici, la fiducia tra gli attori coinvolti è di importanza fondamentale per realizzare prodotti di alta qualità. Questo significa fiducia nella qualità del lavoro ma anche nel corretto funzionamento e integrità dell'intera unità elettronica. Il segreto per stabilire questa fiducia in una rete di produttori e fornitori risiede nel copiare fedelmente la produzione e il processo di commissioning in una Catena di Fiducia (CoT) crittograficamente sicura. Funziona registrando i singoli step produttivi e specifici tratti dei componenti hardware in un dataset protetto e condiviso situato sullo stesso dispositivo, che può essere letto e verificato a livello crittografico in ogni momento durante la produzione o l'utilizzo.
In the distributed manufacturing of electronic systems, trust between the actors involved is of paramount importance for producing high-quality components. This means trust in the quality of work itself and trust in the correct functioning and integrity of the entire electronic unit. The secret to establish such trust in a network of makers and producers lies in mirroring the production and commissioning process in a cryptographically secure Chain of Trust (CoT). It works by recording individual processing steps and specific traits of the hardware components as a shared, protected dataset on the component itself to be read out and cryptographically checked at any time during production or use.



SE con NFC e harvesting energetico su un PCB.
SE with NFC and energy harvesting on a PCB.

SE con CoT sulla scheda di R&S.
SE with CoT on the R&D board.

NUOVE, AFFIDABILI FUNZIONALITÀ CON CODEMETER

Quando un componente elettronico viene messo in servizio, una sequenza di bit unica (UID) viene salvata come caratteristica forte in un record della CoT. Altre caratteristiche fisiche di un sistema elettronico o di determinati componenti vengono testate all'interno del progetto di ricerca per la loro idoneità come caratteristiche aggiuntive di un DID univoco ed identificabile.

Le caratteristiche selezionate formano un'impronta digitale, che a sua volta viene memorizzata come record nella CoT dell'SE. Wibu-Systems sta sviluppando una nuova struttura di dati universali (UvD) per la sua tecnologia di gestione licenze CodeMeter, che consentirà di memorizzare la CoT nell'hardware CodeMeter (CmDongle). Questo nuovo formato dovrebbe permettere flessibilità in termini di quantità e contenuto dei dati da memorizzare e facilitare ulteriori processi di firma e di convalida, anche con lunghezze di chiave fino a RSA 4096 bit e ECC 521 bit. I CmDongle possono anche essere forniti con memoria flash o semplicemente in formato VQFN32; le interfacce includono USB, SPI e schede di memoria.

I record della CoT sono memorizzati nelle voci UvD, insieme a un elenco di certificati del produttore, incluse le relative chiavi pubbliche. Per una gestione delle chiavi private in massima sicurezza, i CmDongle usati per firmare i record dispongono anche di funzioni interne di generazione delle chiavi.Per un livello di sicurezza aggiuntivo, è possibile abilitare la crittografia punto-punto tra il CmDongle e il controllore della macchina o l'operatore. Con i dati contenuti nel record, la CoT può anche essere letta localmente in qualsiasi momento tramite le voci UvD di CodeMeter e convalidata crittograficamente. Questo garantisce l'integrità e l'autenticità dei dati e quindi anche l'affidabilità del componente hardware.

SICUREZZA INTEGRATA NEL PROCESSO DI AVVIO

Un altro importante elemento dell'architettura di sicurezza è una validazione interna automatica della CoT al boot di sistema, che funge da gatekeeper. In questo caso, l'SE (CmDongle) è responsabile di un processo di avvio multi-stadio e controlla l'integrità di ogni record della CoT, prima che il sistema di destinazione e le applicazioni possano avviarsi in sequenza.

La procedura proposta può essere eseguita anche a livello pre-boot del processore principale di un componente. La CoT viene letta e convalidata crittograficamente sull'SE. Quando si utilizzano record di avvio affidabili, ad esempio UIDs, un challenge viene recuperato dall'SE e, ad esempio, inoltrato ad un PUF (una funzione fisicamente non clonabile) ed elaborato; la risposta richiesta viene poi rinviata all'SE e verificata. Questa procedura può essere utilizzata anche per controllare varie caratteristiche fisiche di un componente. Allo scopo, il record della CoT associato viene prima letto dall'SE e convalidato con il certificato associato. La procedura descritta nel record viene quindi eseguita per controllare la caratteristica.

Un altro SE di Wibu-Systems, CmASIC, viene utilizzato nel progetto per dimostrare l'ampia gamma di opzioni hardware e software.

UNA FAMIGLIA DI SUCCESSO

CodeMeter di Wibu-Systems è la pluripremiata famiglia di soluzioni di sicurezza atte a monetizzare il know-how digitale, proteggendo i beni digitali e distribuendoli tramite modelli di licenza versatili. Utilizzando metodologie di crittografia ed offuscamento all'avanguardia e focalizzandosi sull'interoperabilità tra gli elementi software, hardware e cloud dell'universo CodeMeter, la tecnologia supporta la crescita di tutte le imprese, indipendentemente dal settore in cui operano.

Se la convalida della CoT o un controllo delle caratteristiche (impronta digitale) fallisce, possono essere applicate diverse restrizioni, come il reset del sistema hardware, limitazioni delle risorse o il blocco licenze. Questi meccanismi consentono di testare le caratteristiche hardware in un SE hardenizzato (CmDongle), verificare i risultati del test e poi influenzare il processo di avvio in risposta a un risultato positivo o negativo.

Trusted, Digital Identities

The PCB industry is multiplying its efforts to reduce the environmental impact. This involves not only technology, but all corporate activities, with strong impact also on ethics and governance. The European regulations that prescribe strict market standards are driving this transformation. Let's see how some market leaders have started their journey.

The many challenges inherent in the manufacture of complex electronic systems have been exacerbated by a strained supply chain and an increasing number of cyber-threat scenarios that affect the trustworthiness of electronic components and thus the reliability of the equipment that embed them.
The VE-ASCOT R&D project, coordinated by Wibu-Systems and involving Siemens, Infineon, Schölly Fiberoptic, Revisionone Engineering, Fraunhofer Institute SIT, and Kastel Security Labs, aims to create a digital identity (DID) for electronic systems. This DID is a blockchain-based series of data records that document the lifecycle of an electronic component in chronological order. Known as the "Chain of Trust" (CoT), these secure and interconnected records are designed to be constantly accessible, verifiable, and expandable.

ANCHORING TRUST: THE FIRST LINK IN THE CHAIN

The CoT begins with a cryptographic trust anchor consisting of a secret, asymmetric key and an associated certificate, the authenticity of which can be verified at any time. The CoT should be stored in a secure element (SE), which is protected against cyber-attacks. With its serial number and the additional data that are hashed and signed, this original certificate represents the first data record in the CoT, making it the trust anchor and one element of the DID.
All subsequent steps, from production to commissioning, operation, and maintenance of the system, can be integrated into the CoT as data records. Customs or certification data records could be integrated as well, even by means of cryptographic hash values that protect references to external records. Each data record of the CoT is cryptographically secured by a signature, using a public key infrastructure (PKI) that includes, for example, manufacturer, machine or operator certificates. Over time, the CoT in the SE grows, with each record creating an increasingly detailed identity of the electronic system that can be validated at any time, enabling local and independent verification of the trustworthiness of the systems. Feedback responses can also generate records themselves. To better protect the SE, it can also be integrated into the PCB. With a thickness of 1.6 and 1.1 mm, PCBs, equipped with an internal NFC antenna and using energy harvesting to operate the SE, allow for the preset DID to be read out wirelessly.
Copies of the CoT can also be stored in a cloud making it possible to e.g. control the rollout of updates for entire industrial plants from a cloud or mapping components and machines in digital twins.

NEW AND TRUSTWORTHY FEATURES WITH CODEMETER

When an electronic component is commissioned, a unique bit sequence (UID) is saved as a strong feature in a record of the CoT.
Other physical characteristics of an electronic system or

CmDongle per firmare i record e CmDongle per memorizzare un CoT.
CmDongle to sign records and CmDongle to store a CoT.

certain components are also tested as part of the research project for their suitability as additional characteristics for a unique and identifiable DID.
The selected features form a fingerprint, which in turn is stored as records in the CoT of the SE. Wibu-Systems is developing a new Universal Data (UvD) structure for its CodeMeter license management technology that would allow the CoT to be stored in the CodeMeter hardware (CmDongle). This new format should allow flexibility in the amount and content of data to be stored and facilitate additional signing and validation processes, even with key lengths of up to RSA 4096 bit and ECC 521 bit.
CmDongles can also come with flash memory or simple VQFN32 package and various USB, SPI, and card interfaces. The CoT records are stored in the UvD entries along with a list of manufacturer certificates, including the associated public keys. The CmDongles used to sign the records also have internal key generation functions. This provides maximum security for a private key in the CmDongle. For additional security, point-to-point encryption can be enabled between the CmDongle and the machine controller or operator.
With the data contained in the record, the CoT can also be read out locally at any time via the CodeMeter UvD entries and validated cryptographically. This guarantees the integrity and authenticity of the data and therefore also the trustworthiness of the hardware component.

SECURITY INTEGRATED INTO THE BOOT PROCESS

Another important building block in the security architecture is an automatic, internal validation of the CoT at system startup, which acts as a gatekeeper. In this case, the SE (CmDongle) is responsible for a multi-stage boot process and checks the integrity of each record of the CoT before the target system can boot up and applications started.

A SUCCESSFUL FAMILY

CodeMeter by Wibu-Systems is the company's award-winning family of product security solutions that monetize the know-how of any software-powered business by safeguarding their digital assets and distributing them via versatile licensing models. Using cutting-edge encryption and obfuscation methods and an underlying interoperability approach that embraces all the software, hardware, and cloud elements of CodeMeter's universe, the technology is supporting business growth across all verticals.

The proposed procedure can also be executed at the pre-boot level of a component's main processor. The CoT is read and cryptographically validated on the SE. When using trusted boot records, e.g. UIDs, a challenge is retrieved from the SE and e.g. forwarded to a PUF (a Physical Unclonable Function), processed and the required response is sent back to the SE and checked. This procedure can also be used to check various physical characteristics of a component. To do this, the associated CoT record is first read from the SE and validated with the associated certificate. The procedure described in the record is then carried out to check the feature.
Another SE from Wibu-Systems, CmASIC, is also used in the project to demonstrate a range of options for influencing the hardware and software components.
If the validation of the CoT or a feature check (fingerprint) fails, several restrictions, such as hardware system reset, resource restrictions, and blocked licenses, can be applied.
These mechanisms make it possible to test hardware characteristics in a specially hardened SE (CmDongle), verify the results of the test and then influence the boot process in response to a positive or negative result.