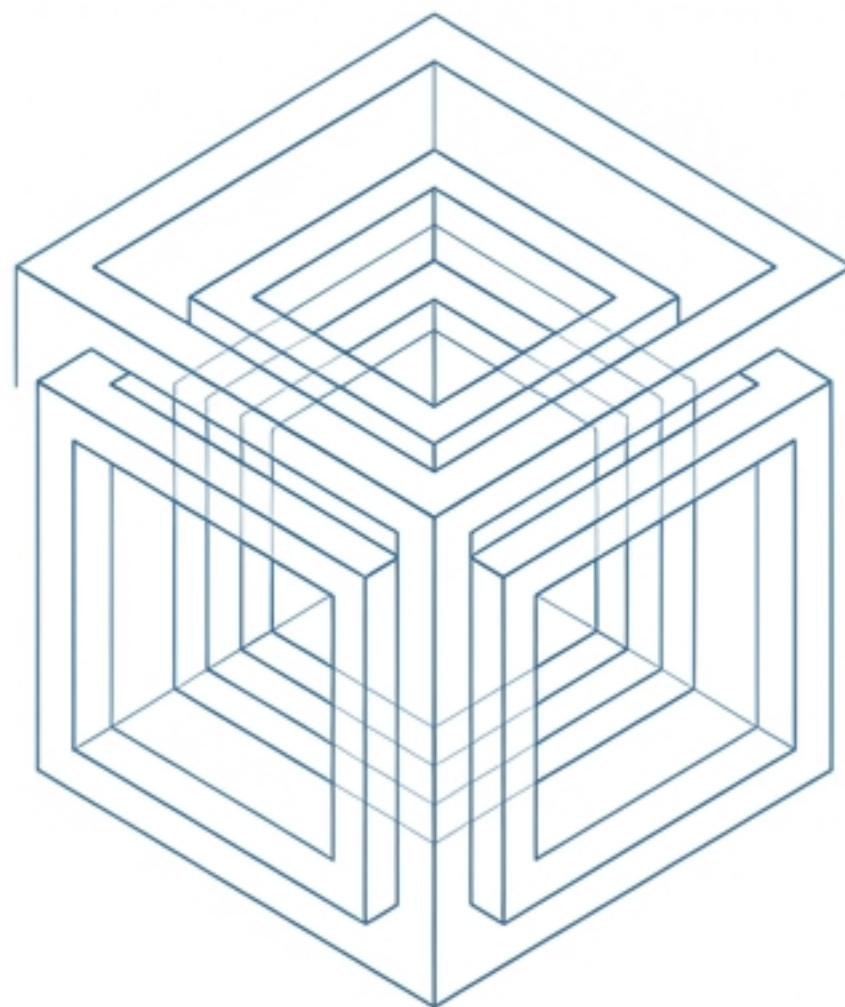




ISO/IEC 15408: CRITERI COMUNI PER LA SICUREZZA IT

Un'analisi strutturale della norma, dei processi di valutazione e dei livelli di certificazione (EAL).

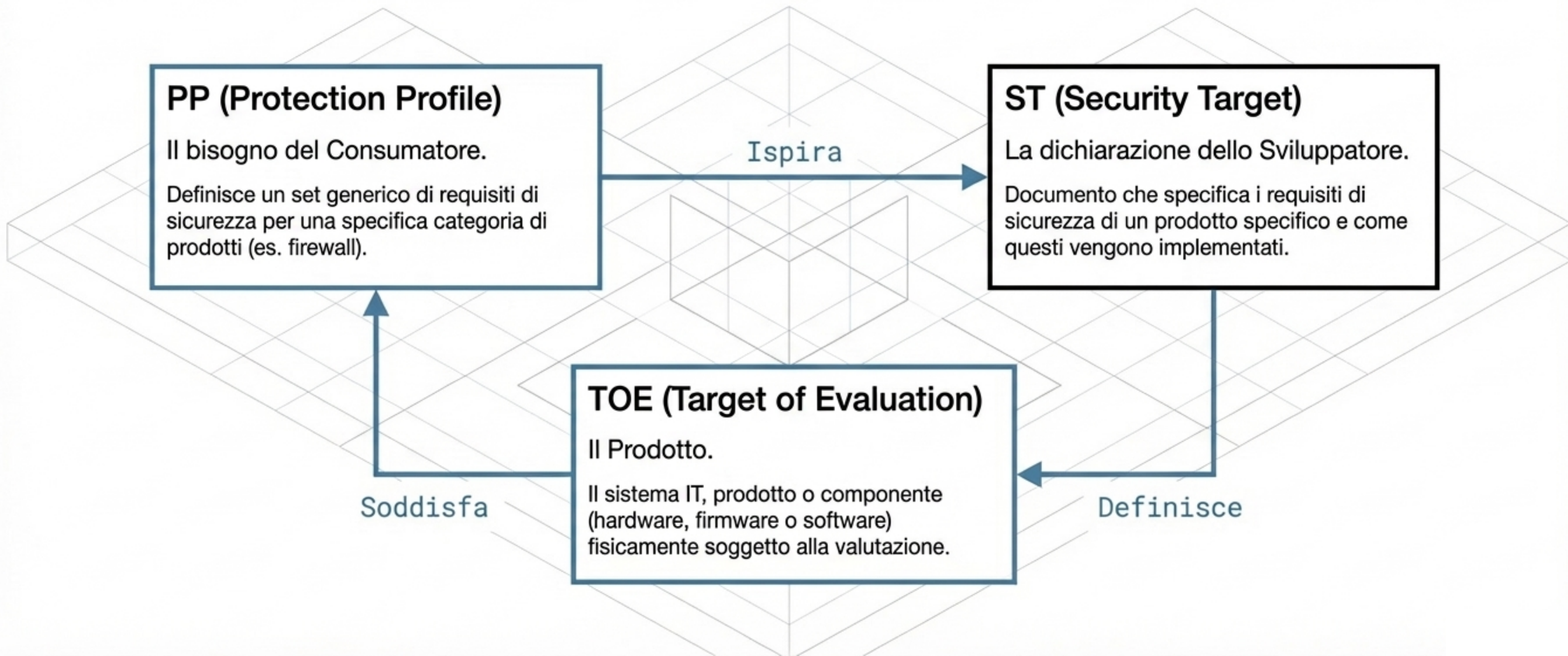
L'Ecosistema ISO/IEC 15408 (Edizione 2022)

La norma garantisce la comparabilità dei risultati delle valutazioni di sicurezza indipendenti attraverso un framework diviso in 5 parti.



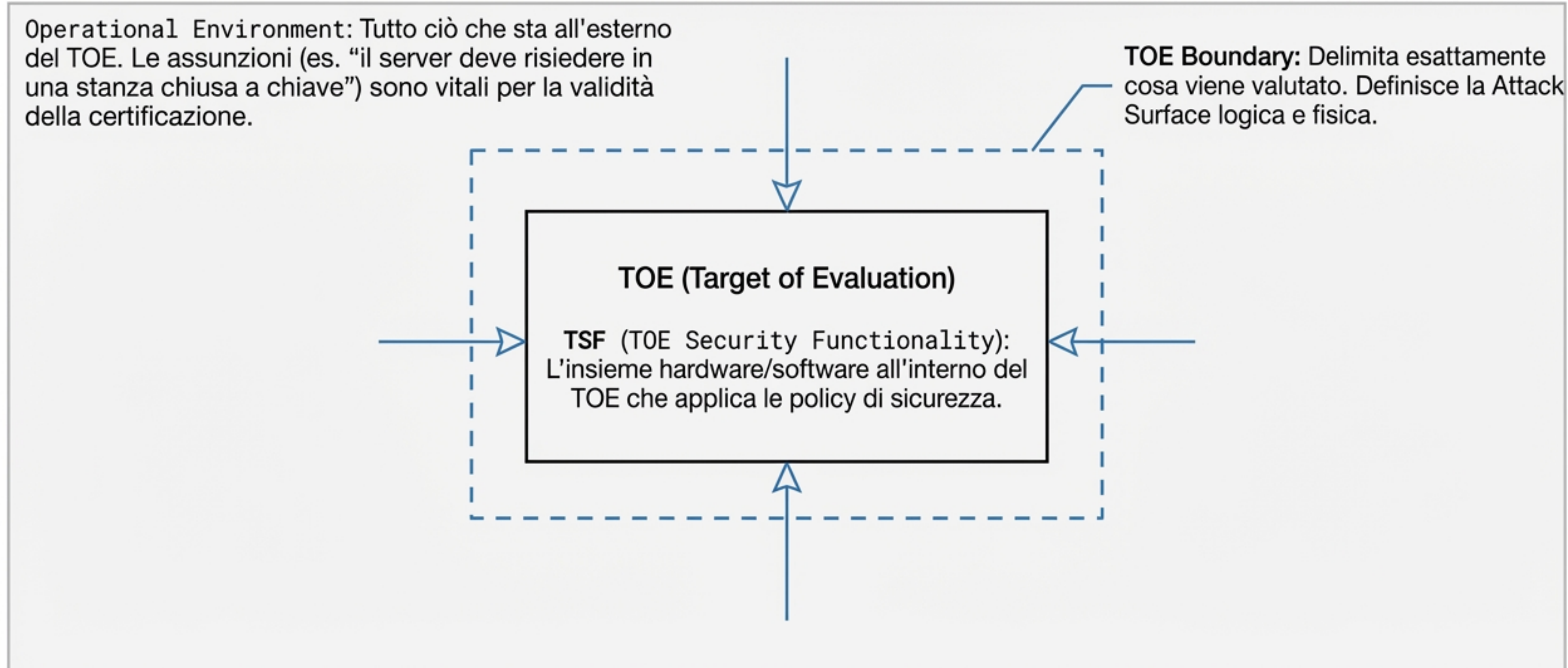
Il Paradigma Fondamentale: TOE, PP e ST

La certificazione è il processo che verifica se un prodotto (TOE) soddisfa le dichiarazioni di sicurezza (ST) per rispondere a specifiche esigenze (PP).



Anatomia del Target of Evaluation (TOE)

La sicurezza non è mai assoluta; è delimitata dai confini fisici e logici del TOE e dipende dal suo ambiente operativo.



I Due Pilastri: Requisiti SFR vs. SAR

Il Part 2 definisce le funzioni di sicurezza del prodotto; il Part 3 definisce il rigore con cui queste funzioni sono state testate e verificate.

SFR

Security Functional Requirements
(Part 2)

- Definizione: "Cosa fa il TOE".
- Natura: Comportamenti attivi e meccanismi tecnici del sistema.
- Esempi: Crittografia, controllo degli accessi, identificazione utente, audit dei log.

SAR

Security Assurance Requirements
(Part 3)

- Definizione: "Quanto bene lo fa".
- Natura: Misure applicate durante lo sviluppo e la valutazione per infondere fiducia.
- Esempi: Profondità dei test, analisi delle vulnerabilità, gestione del ciclo di vita.

Anatomia delle Classi Funzionali (Part 2 – SFR)

Il Part 2 fornisce un catalogo modulare e standardizzato per costruire le specifiche funzionali (ST/PP) senza ambiguità.

FAU

Security Audit

Generazione, analisi e protezione dei log di sicurezza.

FCS

Cryptographic Support

Gestione delle chiavi e operazioni crittografiche (es. AES, RSA).

FDP

User Data Protection

Politiche di controllo degli accessi e flusso delle informazioni.

FIA

Identification & Authentication

Prova di identità, vincoli utente-soggetto.

FPT

Protection of TSF

Sicurezza intrinseca del sistema (es. self-test, fail secure).

Anatomia delle Classi di Assurance (Part 3 - SAR)

Le classi SAR valutano la documentazione, i processi di sviluppo e la resistenza agli attacchi, formando la base per i livelli EAL.

ADV

Development

Architettura, design modulare e implementazione del TSF.

ALC

Life-cycle Support

Configuration management, sicurezza dell'ambiente di sviluppo e flaw remediation.

ATE

Tests

Copertura, profondità e test funzionali indipendenti.

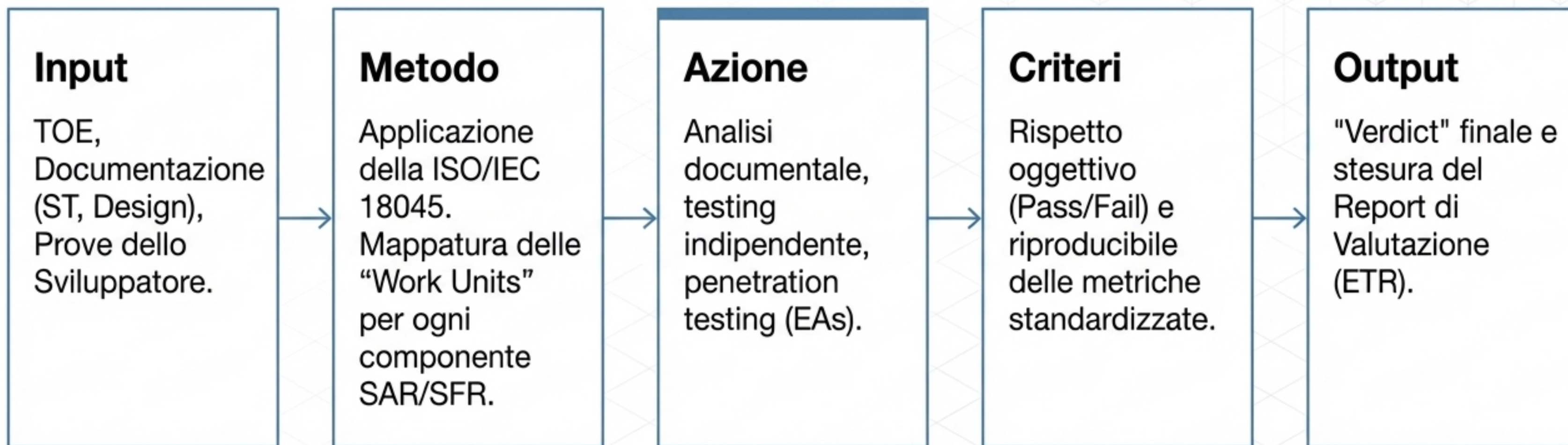
AVA

Vulnerability Assessment

Analisi metodica delle vulnerabilità e penetration testing.

La Metodologia e il Processo di Valutazione (Part 4)

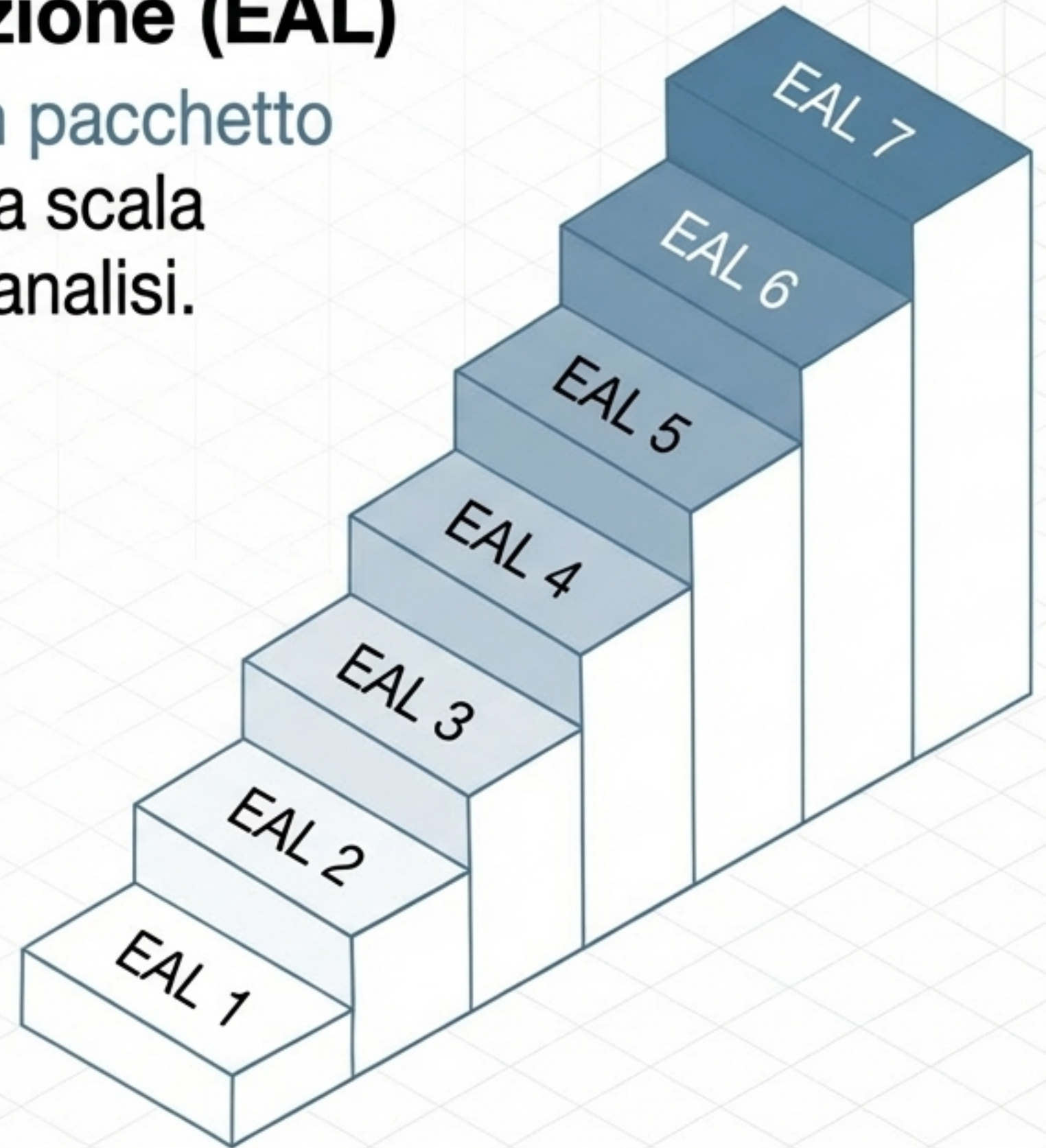
I valutatori non improvvisano; derivano EAs (Evaluation Activities) rigorose dalle unità di lavoro definite nella metodologia ISO/IEC 18045.



Introduzione ai Livelli di Certificazione (EAL)

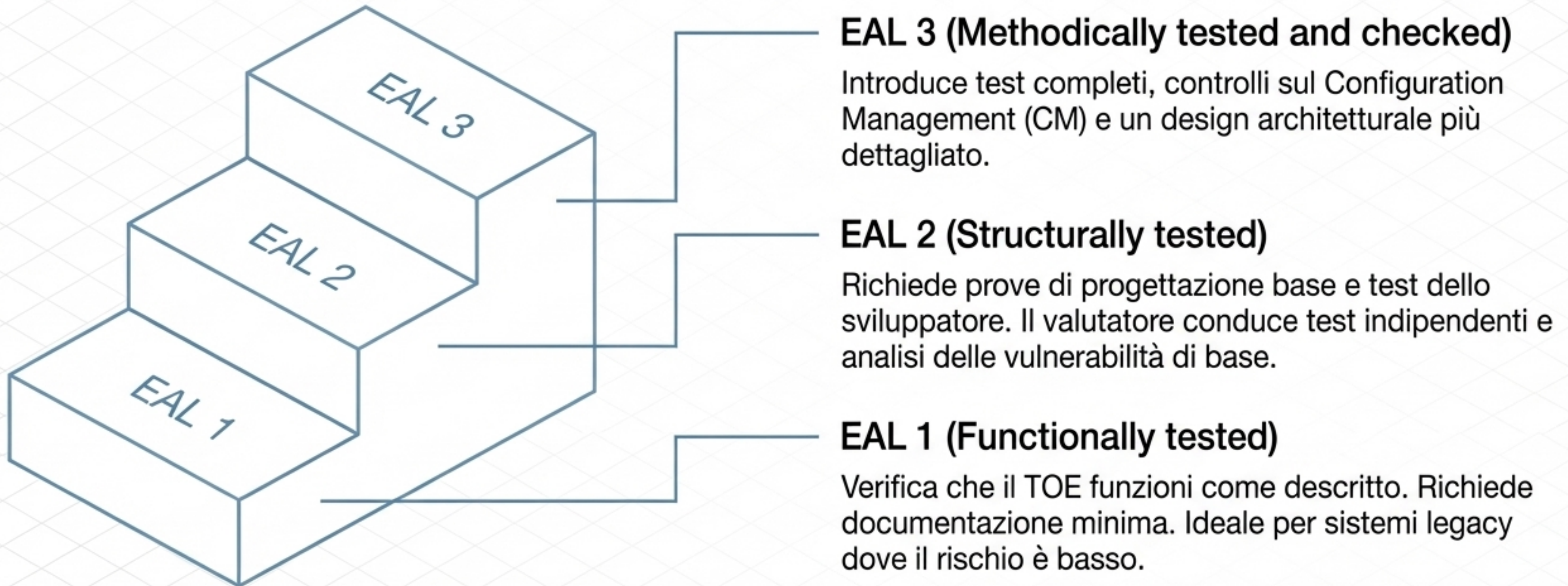
Un EAL (Evaluation Assurance Level) è un pacchetto predefinito di requisiti SAR disposti su una scala crescente di rigore, costo e profondità di analisi.

- I livelli vanno da EAL1 (test funzionali di base) a EAL7 (verifica matematica formale).
- Salire di livello non significa aggiungere nuove funzioni di sicurezza (SFR), ma aumentare la certezza che le funzioni esistenti siano implementate senza vulnerabilità.
- La scelta dell'EAL è un compromesso tra il livello di rischio accettabile e il costo della certificazione.



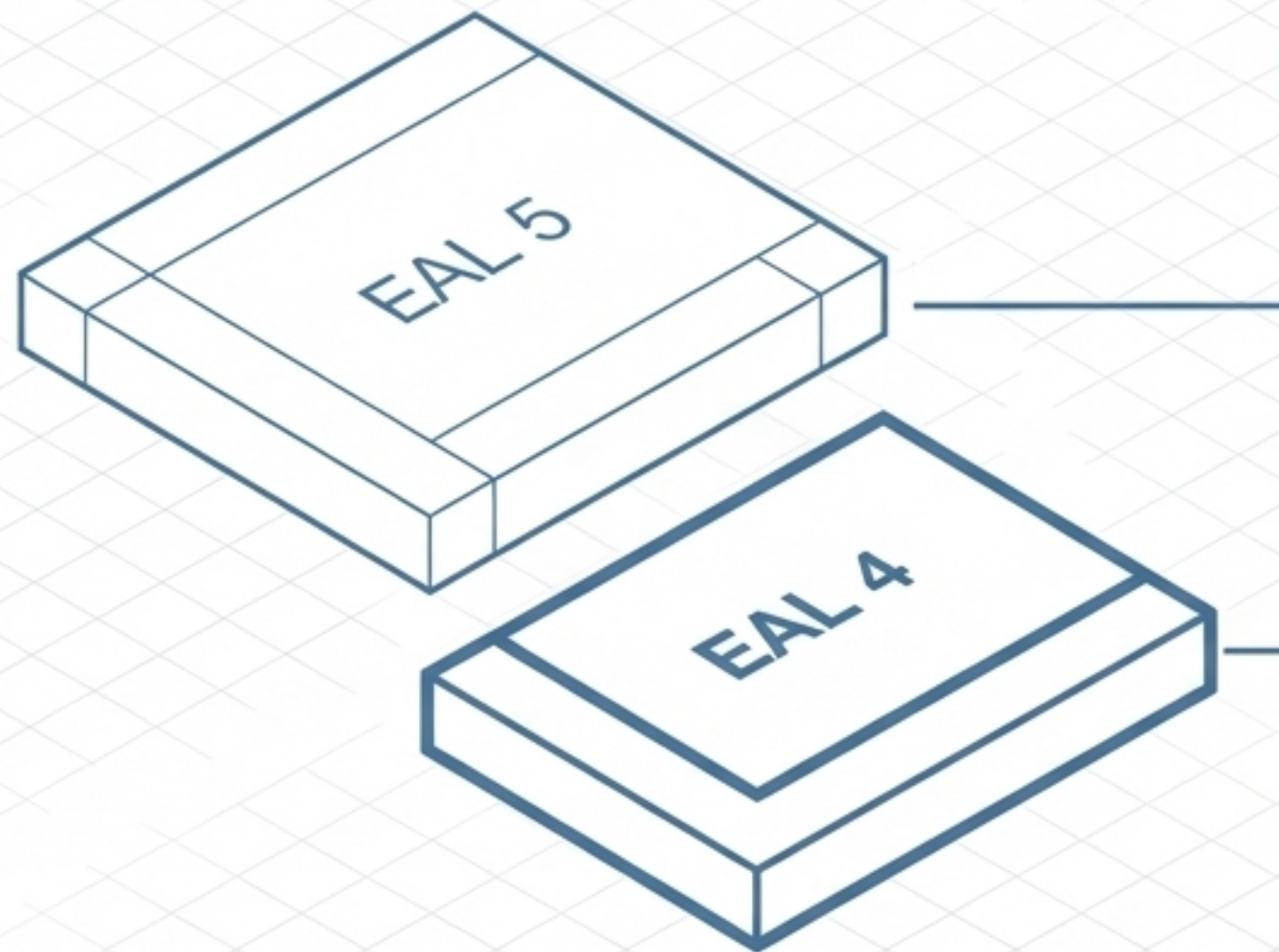
EAL 1-3: Test Strutturali e Metodici

I primi tre livelli si concentrano sull'analisi black-box e gray-box, fornendo fiducia senza richiedere una riprogettazione del prodotto.



EAL 4-5: Progettazione e Verifica Semi-Formale

L'EAL 4 rappresenta il livello massimo di certificazione economicamente fattibile per lo sviluppo di software commerciale complesso.



EAL 5 (Semi-formally verified design and tested)

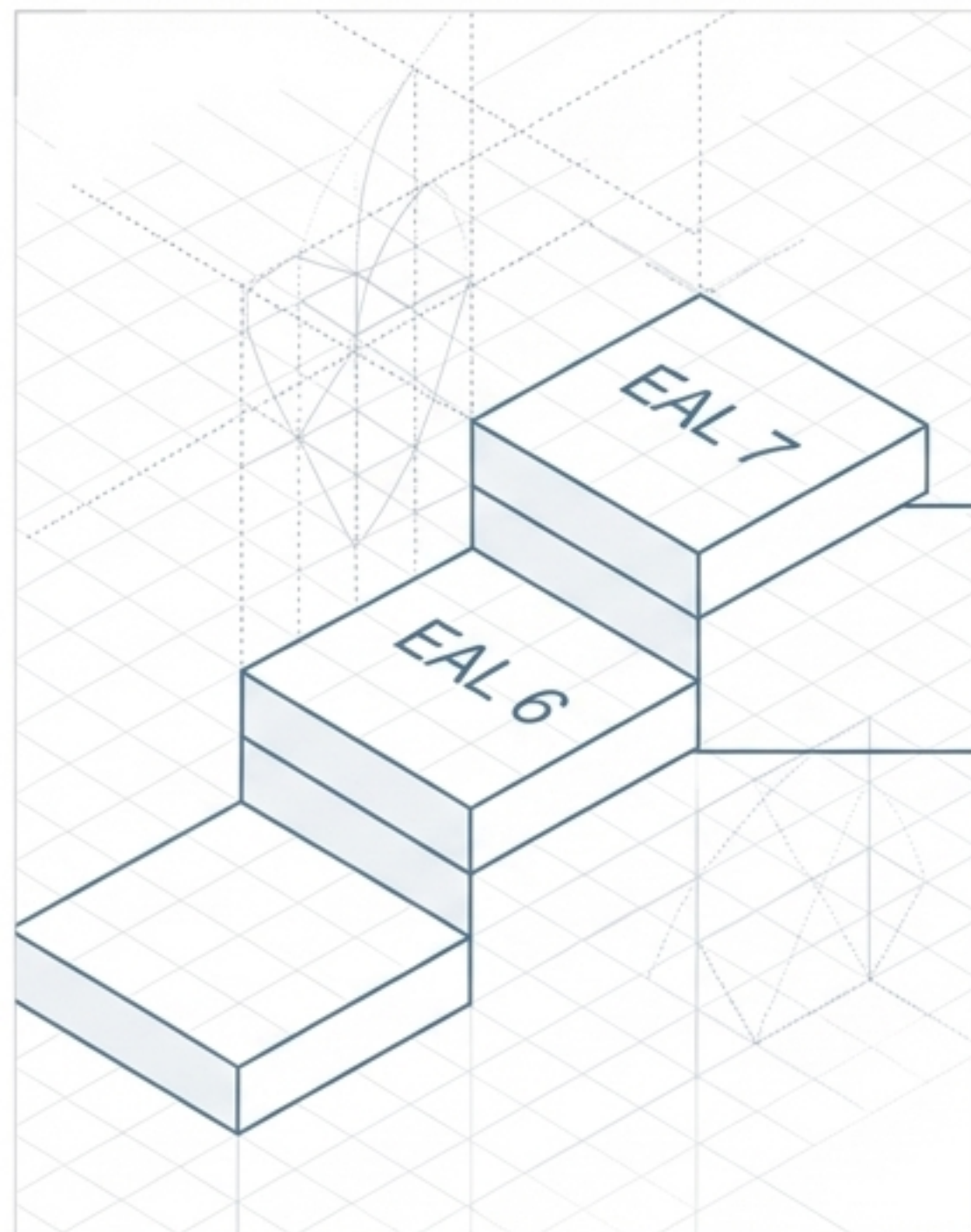
Applica un design semi-formale e un'architettura rigorosamente strutturata. Rivolto ad applicazioni ad alto rischio (es. smart card) dove la sicurezza ingegneristica supera le pratiche commerciali standard.

EAL 4 (Methodically designed, tested, and reviewed) - LO STANDARD COMMERCIALE

Richiede l'accesso al codice sorgente, un rigoroso isolamento del TSF e un'analisi completa delle vulnerabilità (AVA_VAN.3). Tipico di Sistemi Operativi e Firewall enterprise.

EAL 6-7: Rigore Assoluto e Verifica Formale

Riservati ad ambienti ostili ad altissimo rischio (militare, aerospaziale), questi livelli richiedono che la sicurezza sia provata matematicamente.



EAL 7 (Formally verified design and tested)

Richiede rappresentazioni matematiche e formali del TOE Security Policy Model (ADV_SPM).

Praticabile solo per sistemi con un raggio d'azione estremamente ristretto e controllato (es. microkernel sicuri o hardware crittografico dedicato).

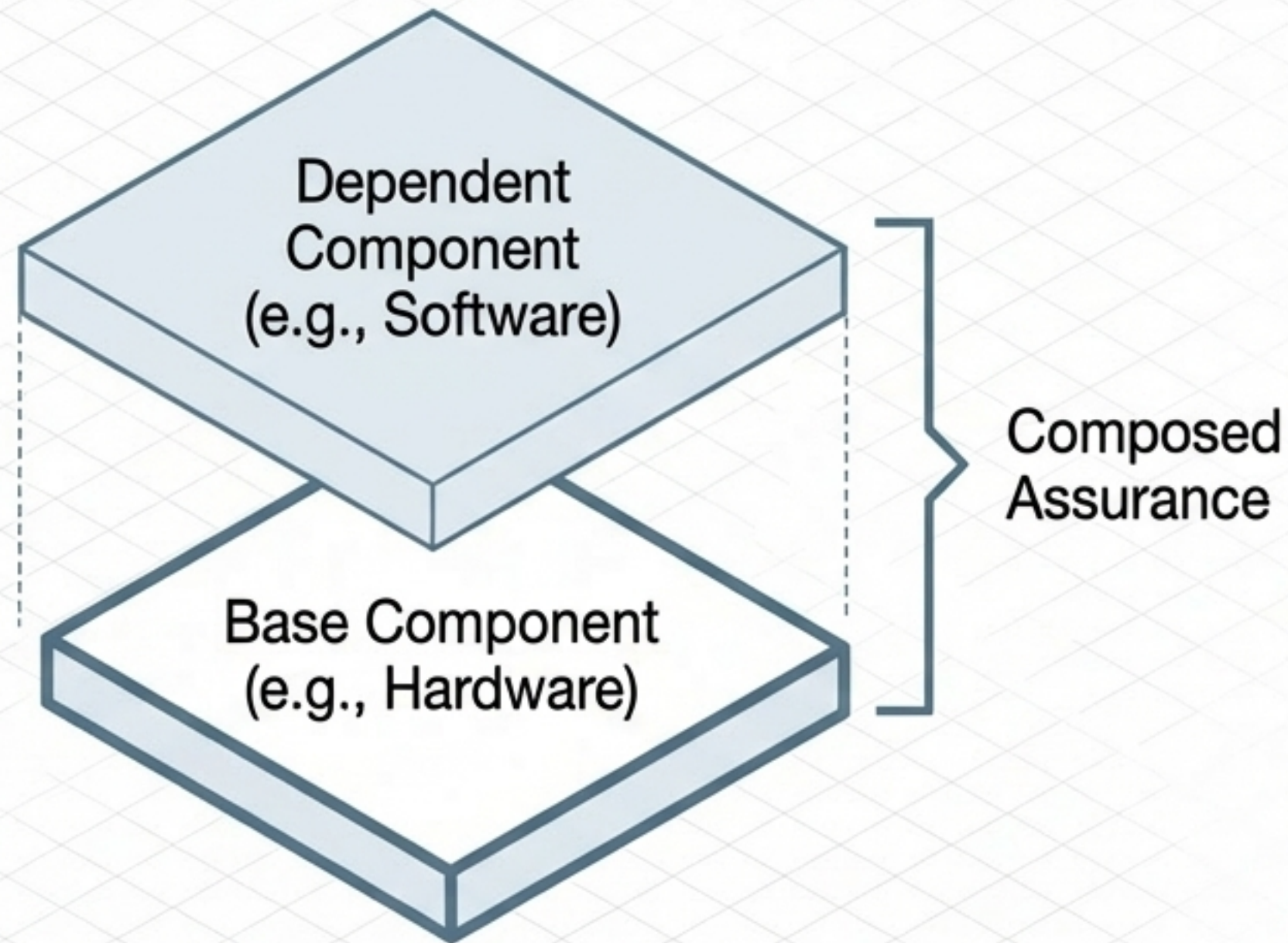
EAL 6 (Semi-formally verified design and tested)

Sviluppo in un ambiente fisicamente e logicamente protetto.

Test di penetrazione avanzati (AVA_VAN.5) contro attaccanti con altissimo potenziale offensivo (High Attack Potential).

La Composizione dell'Assurance (CAP e COMP)

I sistemi IT moderni sono stratificati. ISO 15408 permette di riutilizzare le valutazioni di componenti base per certificare prodotti composti.



Base TOE: Un componente indipendente già valutato (es. un microchip).

Dependent TOE: Un componente che si appoggia ai servizi del Base TOE.

ACO (Composition Class): Valuta in modo specifico le interazioni tra i due componenti.

CAP (Composed Assurance Packages): Una scala predefinita (A, B, C) per certificare sistemi composti, evitando di dover ri-valutare da zero l'intero stack tecnologico.

Matrice di Sintesi dell'Assurance

La progressione degli EAL non è arbitraria, ma è una scalata incrementale della profondità analitica e del rigore procedurale.

				↙ Jump in attack resistance			
AVA_VAN (Vulnerabilità)	1	2	2	3	4	5	5
ADV_FSP (Specifica Funzionale)	1	2	3	4	5	5	6
ATE_IND (Test Indipendenti)	1	2	2	2	2	2	3
	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7

Conclusione: Il Vero Significato della Certificazione

La certificazione ISO/IEC 15408 non garantisce che un prodotto sia 'inviolabile'. Garantisce, con un livello di confidenza misurabile (EAL), che il prodotto rispetta le specifiche dichiarate (ST) contro le minacce previste (PP).

Il Contesto Regna

Un EAL alto su un Security Target debole è inutile. Il vero valore risiede nella combinazione tra rigore (SAR) e funzionalità adeguata (SFR).

Standardizzazione

Fornisce un linguaggio universale (es. FAU, FDP, ADV) che permette a governi e aziende di confrontare in modo oggettivo soluzioni IT concorrenti.

Evoluzione Continua

Con l'introduzione dei pacchetti modulari e le valutazioni composte (CAP), l'edizione 2022 si adatta agilmente alle moderne architetture cloud e IoT.