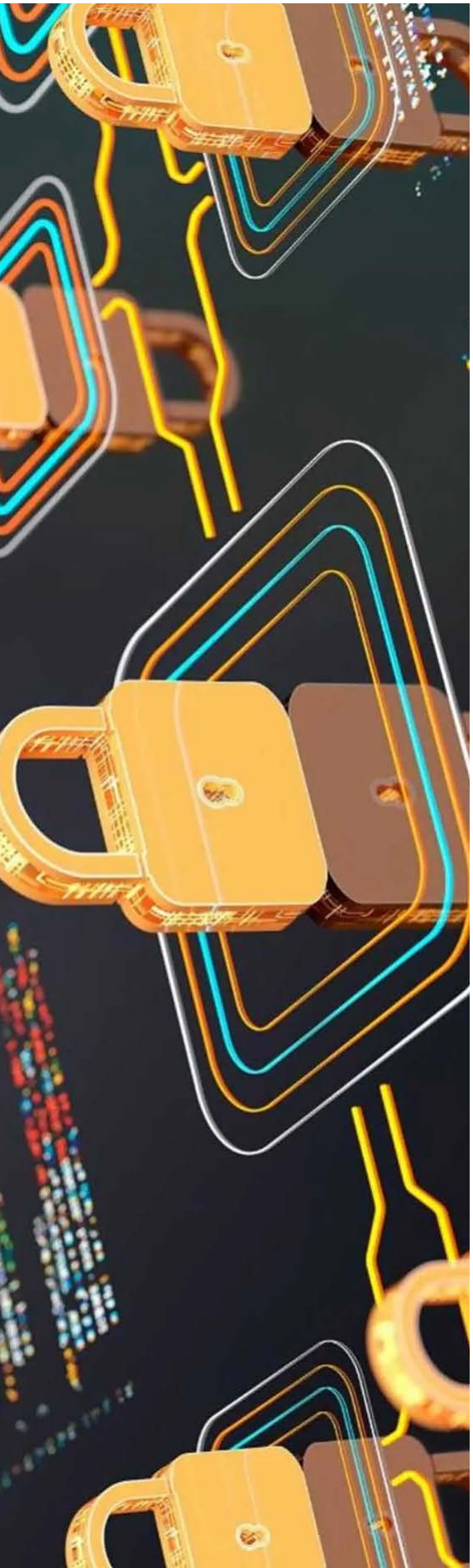
Security Levels: cosa sono e perché sono importanti per la sicurezza dei prodotti in ambito OT

Testi a cura di

Andrea Razzini

LEGGI SUL SITO



INDICE DEGLI ARGOMENTI

Fin dalle prime fasi di progettazione di un prodotto/sistema in ambito OT (Operational Technology) occorre eseguire una attività fondamentale di analisi delle minacce e calcolo del rischio, per stabilire asset, scenari di minaccia, potenziali vulnerabilità e vettori di attacco. Ecco cosa sono e come identificare i Security Levels

Uno degli obiettivi importanti della cyber security in ambito OT (Operational Technology) è riuscire a determinare l'insieme dei requisiti che in fase di progetto verranno implementati per mettere in sicurezza oggetti, prodotti, componenti hardware e software, sistemi e connettività.

Questo insieme di requisiti deve essere determinato in base ad alcune considerazioni che sono alla base del concetto di Security Level:

- tipologia di attaccanti da cui è necessario proteggersi;
- contesto in cui il prodotto sotto esame è inserito e il modo in cui funzionerà: in autonomia o isolato o con collegamenti verso altri sistemi/entità;
- garanzia che si vuole ottenere in sede di eventuale certificazione;
- livello di maturità di partenza dell'azienda il cui prodotto è oggetto della progettazione security by design;
- valutazione corretta del rischio connesso all'utilizzo di quel dato prodotto in termini di cyber security.

1

COSA SONO I SECURITY LEVELS

Nel mondo della Safety esiste già un concetto di Safety Integrity Levels (SIL), ovvero di rappresentare con un numero in una certa scala, un fattore di protezione necessario per garantire la sicurezza delle persone , dell'ambiente in cui si muovono e dei loro elementi di valore (assets).

Nella cyber security vale un concetto molto simile in cui il fattore di protezione viene determinato come visto in precedenza riferendosi ad uno scenario di possibile cyber attacco. In questo senso, la complessità diventa molto ampia e l'esperienza personale nonché l'applicazione di standard e best practice sono gli aspetti che devono guidare nella determinazione di questo numero.
Una volta stabilito il livello più appropriato di sicurezza del prodotto/sistema, sarà più facile stabilire l'insieme dei requisiti da applicare in fase di security by design, con complessità e difficoltà di implementazioni crescenti.

Questa mappatura tra requisiti e Security Levels è contenuta nei documenti che fungono da standard di riferimento dei vari settori industriali del mondo OT (Operational Technology).
Gli standard principali della cyber security che consideriamo nel seguito e che contengono linee guida su come procedere a calcolare i Security Levels, sono:

- IEC 62443 per il mondo ICS (Industrial Control Systems);
- ISO 21434 per il settore automotive;
- CENELEC 50701 per il settore ferroviario;
- ISO 15408 per un generico prodotto IT/OT.

Vedremo nel seguito definizioni e differenze tra di essi.

2. I SECURITY LEVELS PER IL SETTORE INDUSTRIALE

In questa generica definizione di "industriale" rientrano i prodotti appartenenti alle aziende che a loro volta fanno parte del settore denominato Industry4.0, ma anche del Industrial Control Systems, Smart Buildings, Energy, Life Sciences (Medical Devices) e via dicendo.

Lo standard che guida tutti questi settori è IEC 62443.

Nello standard sono innanzitutto definiti 3 diversi tipi di Security Levels:

1. SL-T:è il livello "Target", ovvero il livello desiderato di sicurezza per un certo prodotto, calcolato durante la fase di Risk Assessment;
2. SL-C:è il livello "Capability", ovvero quello fornito dal prodotto una volta configurato. Questi livelli indicano che un particolare componente o sistema è in grado di soddisfare gli SL target in modo nativo senza ulteriori contromisure compensative quando correttamente configurato e integrato;
3. SL-A: è il livello "Achieved", ovvero il livello effettivo raggiunto da un certo prodotto. Dopo un opportuno Assessment sul prodotto, questo valore SL-A dovrà essere confrontato con il valore SL-T.

Questi Security Levels hanno 5 diversi valori nello standard IEC 62443, da 0 a 4, con livelli che si incrementano nel modo seguente:

1. SL0: Non sono necessari requisiti specifici o protezione di sicurezza;
2. SL1: Protezione contro violazioni casuali;
3. SL2: Protezione contro la violazione intenzionale utilizzando mezzi semplici con basso livello di

esperienza delle risorse coinvolte, competenze generiche e scarsa motivazione;
4. SL3: Protezione contro la violazione intenzionale utilizzando mezzi sofisticati con risorse moderate, competenze specifiche su Industrial Control Systems e motivazione moderata;
5. SL4: Protezione contro la violazione intenzionale utilizzando mezzi sofisticati con risorse estese, competenze specifiche su Industrial Control Systems ed elevata motivazione.

Lo standard contiene poi le tabelle di mappatura tra requisiti e Security Levels Capability (SL-C) in base a questi 5 livelli.

Come esempio prendiamo il requisito dello standards IEC 62443 relativo alla autenticazione degli utenti:
1. SL1: ho solo il requisito che impone l'obbligo di identificare e autenticare tutti gli utenti;
2. SL2: al requisito precedentesi deve aggiungere l'obbligo di identificare e autenticare tutti gli utenti "in modo univoco";
3. SL3: al requisito precedente si deve aggiungere l'obbligo di identificare e autenticare tutti gli utenti utilizzando una Multi Factor Authentication (MFA) sulle reti considerate non-fidate (untrusted);
4. SL4: al requisito precedente aggiungo l'obbligo di identificare e autenticare tutti gli utenti utilizzando una Multi Factor Authentication (MFA) su tutte le reti.

Come si vede dall'esempio, al crescere del Security Level, aumenta la complessità e numerosità dei requisiti da prendere in considerazione. Il Security level diventa misura della protezione che si vuole ottenere ma anche contemporaneamente misura del rischio associato ad un certo prodotto.

3. I SECURITY LEVELS PER IL SETTORE AUTOMOTIVE

I Security Levels dello standard ISO 21434 che guida la cyber security del mondo Automotive sono meglio noti come CAL (Cybersecurity Assurance Levels).

Una CAL può essere utilizzata per specificare una serie di requisiti di garanzia, in termini di livelli di rigore o impegno, per garantire che la protezione delle risorse sia adeguata.

La CAL non specifica i requisiti tecnici per le misure di sicurezza informatica, la CAL può essere utilizzata per guidare l'ingegneria della sicurezza informatica, fornendo un linguaggio comune per comunicare i requisiti di garanzia della sicurezza informatica tra le organizzazioni coinvolte.

Segue nello standard una linea guida sugli impatti derivanti dalla scelta di un ben preciso valore di CAL.

Una volta determinata, una CAL specifica la quantità di effort richiesta nelle successive attività di sviluppo del prodotto per affrontare scenari di minaccia che richiedono la riduzione del rischio.

Ad esempio in fase di verifica e validazione del prodotto OT, dovrò eseguire test di sicurezza (dal vulnerability scanning al penetration testing) con livelli crescenti di approfondimento dei test se si intende raggiungere progressivamente il livello più alto di CAL4.

4

I SECURITY LEVELS PER IL SETTORE FERROVIARIO

I Security Levels dello standard CENELEC 50701 che guida la cyber security del mondo Ferroviario sono derivati dallo standard IEC 62443. Ritroviamo dunque anche in questo settore i concetti di SL-T, SL-A, SL-C visti in precedenza , ma ci sono delle differenze importanti.
Il valore SL-T viene stabilito durante la fase di Risk Assessment, ma con un doppio passaggio:
risk assessment iniziale e determinazione del valore SL-T iniziale, basandosi molto sull'esperienza personale e/o sulla profilazione degli attaccanti;
scelta delle contromisure da applicare per abbassare il rischio ed eventuale aggiornamento del valore SL-T
ripetizione di questo processo fino ad ottenere un livello accettabile di rischio e il valore finale di SL-T viene fissato definitivamente.
Il valore del SL-T viene poi rappresentato in realtà come un vettore a 7 valori, dove ogni numero di SL-T si riferisce ad uno dei 7 “Foundational Requirements” dello standard IEC 62443 che sono i seguenti:

Identification and authentication control (IAC);

a. Use control (UC);
b. System integrity (SI);
c. Data confidentiality (DC);
d. Restricted data flow (RDF);
e. Timely response to events (TRE);
f. Resource availability (RA).

Ad esempio, per un sistema abbastanza complesso potrò avere un SL-T così definito: [3,3,3,1,3,2,3]. Con l'aiuto dello standard determinerò i requisiti applicabili per la fase di design.

5

I SECURITY LEVELS PER PRODOTTI ICT

La convergenza tra il mondo OT e IT è ormai inarrestabile. Di conseguenza anche gli aspetti di cyber security devono abbracciare entrambi i due ambiti. Il concetto di Security Level nel mondo IT è definito da uno standard noto come Common Criteria.
I Security Levels dello standard ISO 15408 meglio noto come Common Criteria, che guida la Cybersecurity alla certificazione di prodotti IT, sono meglio noti come EAL (Evaluation Assurance Levels).

Per un generico prodotto hardware o software o che comprende entrambe le parti, sono stabiliti 7 diversi livelli: da EAL1 a EAL7, con la seguente importanza in ordine crescente:

1. EAL1: testato funzionalmente;
2. EAL2: testato strutturalmente;
3. EAL3: testato e controllato;
4. EAL4: progettato, testato ed esaminato secondo metodologie;
5. EAL5: progetto semiformale e testato;
6. EAL6: progetto semiformale, verificato e testato;
7. EAL7: progetto formale, verificato e testato.

Come si vede dalle definizioni, questa classificazione è diversa dalle precedenti e intende stabilire come un prodotto è stato progettato, testato e verificato.
Di nuovo poi nello standard si definiscono le tabelle di mappatura tra questi Security Levels e le famiglie di Assurance ovvero di requisiti funzionali che dovranno essere applicati ad ogni livello desiderato.
Un punto importante di questa certificazione è la documentazione a corredo dei vari EAL che si intendono raggiungere.

6. CONCLUSIONI

Fin dalle prime fasi di progettazione di un generico prodotto/sistema occorre eseguire una attività fondamentale di analisi minacce e calcolo del rischio (TARA, Threat Analysis and Risk Assessment). In questa fase vengono stabiliti gli asset, gli scenari di minaccia potenziali, le potenziali vulnerabilità, i possibili vettori di attacco. Vengono calcolati impatti e probabilità dei vari scenari di minaccia ed infine calcolato ogni singolo rischio.

È proprio durante questa attività che è quanto mai importate stabilire anche un Security Level Target. Questo parametro guiderà le scelte successivamente , nella fase di implementazione dei requisiti, stabilendo in modo chiaro quali e quanti requisiti vanno considerati per raggiungere quel livello di sicurezza desiderato e con quale effort, visto che molti requisiti hanno complessità crescente in base al livello stabilito.

Cosa succede per i prodotti cosiddetti “legacy"? spesso molti prodotti del mondo OT sono nati senza fare security by design. Questo significa che diventa molto difficile riuscire ad assegnare un SL-T in base agli standard di riferimento. Si rende quindi necessario fissare un livello minimo di sicurezza che possa proteggere dalla maggior parte dei cyber attacchi, utilizzando ad esempio altre linee guida come la ISO 27001.

Ecco che di nuovo diventa importante coniugare esperienza, conoscenza e best practice di cyber security.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di **Digital360HUB**, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ