

Webinar di aggiornamento professionale

La Cybersecurity per i Sistemi di Controllo Industriale (terza edizione)

21 e 22 Novembre 2023

Obiettivi

Nell'era della digitalizzazione e dell'Impresa 4.0 (già Industria 4.0), le aziende sono diventate sempre più interconnesse perché attraverso l'adozione di servizi industriali basati su Internet e di dispositivi IIoT è stato possibile sviluppare sistemi che consentono di migliorare la gestione degli impianti.

Il processo di trasformazione digitale ha portato ad una significativa sovrapposizione del dominio dei sistemi tipici dell'OT (*Operation Technology*) (sistemi: di controllo di processo, di supervisione, di monitoraggio, anche remoto, di acquisizione, di storicizzazione dei dati ...) con quello dei sistemi informativi tipici dell'IT (*Information Technology*). Fino a qualche anno fa, i sistemi di controllo industriale (IACS, *Industrial Automation Control Systems*) erano progettati con un focus particolare sugli aspetti di sicurezza di impianto (*safety*) e di sicurezza funzionale (*functional safety*), trascurando gli aspetti di sicurezza informatica (*cybersecurity*) perché i domini OT e IT erano disconnessi.

Più recentemente, è aumentata la consapevolezza dell'importanza della sicurezza informatica dei sistemi OT per fronteggiare le sfide che la trasformazione digitale comporta. Nello stesso tempo, si è compreso come i requisiti di *cybersecurity* dei sistemi IACS siano differenti da quelli dei sistemi IT in termini dei potenziali rischi, delle metodologie e delle tecnologie da adottare per attuare le appropriate contromisure di protezione e mitigazione dei rischi. E' in questo scenario che la famiglia degli standard internazionali IEC 62443 gioca un ruolo importante nel definire le specifiche (funzionali e strutturali) che devono esibire i componenti di un sistema IACS (sensori, attuatori, PLC, SCADA ...)

Il seminario si propone di illustrare gli aspetti essenziali degli standard IEC 62443 per aiutare l'operatore a definire le specifiche che deve avere un sistema di gestione efficace della sicurezza cibernetica di una rete di controllo industriale. Il webinar è articolato in due mezze giornate. La prima affronterà gli aspetti metodologici mentre la seconda porrà il focus sugli aspetti pratici tramite la discussione di casi di studio di interesse industriale.

Il webinar è rivolto ai responsabili e agli operatori di impianto, ai responsabili dei sistemi di controllo industriale e di supervisione, ai responsabili di produzione, ai responsabili dei servizi OT e IT.

Il webinar sarà videoregistrato

La partecipazione al webinar potrà essere fatta nelle due modalità: a) diretta *streaming* e b) *on-demand* (agli iscritti verranno inviati i link delle videoregistrazioni).

Coordinatore: Alberto Servida (Università di Genova e Anipla; servida@unige.it)

MODALITÀ DI PARTECIPAZIONE

Piattaforma TEAMS. I link per accedere alle dirette verranno forniti dopo l'iscrizione

CONTATTI

Segreteria ANIPLA - e-mail anipla@anipla.it
tel 02 39289341

ISCRIZIONE ONLINE attraverso la piattaforma Eventbrite: [clicca qui](#)

Con il patrocinio di:



QUOTE DI PARTECIPAZIONE

Il webinar è riservato ai Soci di ANIPLA e delle Associazioni/Organizzazioni che hanno concesso il loro patrocinio (AIDIC, AIS-ISA-Italy Section, GISI e SIRI) per i quali la quota di partecipazione è pari a 150,00 € (richiedere il codice sconto alla Segreteria della propria Associazione/Organizzazione). La quota, include il materiale didattico e l'accesso *on-line* alle videoregistrazioni del seminario. Per i Soci Anipla Junior è prevista la partecipazione gratuita. Per i Soci Collettivi e Sostenitori di Anipla sono previste quote di partecipazione scontate. Per i non soci la quota di partecipazione è di 225,00 € che comprende la quota di adesione ad ANIPLA fino al 31.12.2024. Per i partecipanti alle precedenti edizioni del webinar è stata prevista la possibilità di partecipare solo al secondo modulo al costo di 80,00€.

RINUNCE

In caso di eventuali rinunce non pervenute per e-mail almeno 7 gg prima dell'inizio della manifestazione, sarà trattenuta la quota di partecipazione. La documentazione sarà spedita per e-mail.

Anipla si riserva la facoltà di annullare l'iniziativa o di modificare il programma dandone tempestiva comunicazione.

PROGRAMMA

I MODULO (21 novembre 2023)

9:15 – 9:30 Apertura dei lavori

Enzo Birindelli (Italia Automazione e Presidente Anipla)
Alberto Servida (Università di Genova e Anipla) -
Moderatore

9:30 – 10:45 Luca Casati (H-ON Consulting)

Struttura della norma internazionale IEC 62443

I destinatari della norma e rispettivo ruolo nel processo:
end-user, system integrator, costruttori di componenti e
sistemi, provider

I processi essenziali per *cybersecurity* in ambito
industriale, partendo dall'end user dalla fase di
assessment a quella di mantenimento, passando per
l'implementazione (IEC 62443-2-1).

Analisi e valutazione dei rischi di CS (IEC 62443-3-2).

I requisiti di sicurezza per i sistemi (IEC 62443-3-3) e i
componenti (IEC 62443-4-2)

Il *product development life cycle* per i produttori di sistemi
e componenti (IEC 62443-4-1)

10:45 – 11:00 Risposte alle domande

11:00 – 12:30 Luca Casati (H-ON Consulting)

Dinamica di un attacco cyber

Esempio pratico di come avviene un attacco ai dispositivi
OT

Esempio pratico relativo alla valutazione dei rischi secondo
IEC 62443-3-2

12:30 – 13:00 Risposte alle domande

II MODULO (22 novembre)

9:15 – 9:30 Apertura dei lavori

Alberto Servida (Università di Genova e Anipla)

9:30 – 10:30 Davide Crispino (Phoenix Contact)

Da Stuxnet ai giorni nostri; introduzione all'importanza
della *cybersecurity* nel mondo industriale.

I rischi tipici nelle applicazioni industriali IT Security vs OT
Security: differenze.

Primi approcci alla risoluzione: analisi dei rischi cibernetici
(identificazione: dei componenti critici delle minacce e
delle vulnerabilità) e valutazione delle possibili
conseguenze secondo IEC 62443-2-4.

Mitigazione dei rischi; dalla segmentazione delle reti
(realizzazione dei sistemi di protezione e suddivisione in
celle di produzione) fino al Malware control.

Esempio applicativo.

Importanza del monitoraggio sia dei componenti principali
di una rete industriale produttiva sia degli elementi
principali di una rete di controllo; IPS ed IDS.

10:30 – 11:00 Risposte alle domande

11:00 – 12:30 Davide Crispino (Phoenix Contact)

Un esempio live di attacco hacker ad una tipica network
industriale; individuazione target, scanning delle
vulnerabilità, *brute force*, *man in the middle* fino allo stop
alla produzione.

A titolo esemplificativo si illustreranno *tool* in grado di
recuperare "informazioni critiche" utili per la preparazione
degli attacchi cibernetici (per esempio, Shodan, Password
Dump su Darkweb, ecc.) dando poi una breve panoramica
dei *tool* utili a preparare attacchi simulati (*penetration test*)
da parte degli *Ethical Hacker* e reali da parte dei *Cyber
Criminal*.

Panoramica sulle soluzioni proposte di mitigazione
(hardware e software) per la protezione dell'integrità del
sistema di automazione (PLC, SCADA, ...).

12:30 – 13:00 Risposte alle domande

DOCENTI

Luca Casati
H-ON Consulting

Davide Crispino
Phoenix Contact

Media partner