Cyber Physical Systems

Panoramica sulla sicurezza

Bianca Crippa

2021

Argomenti

Cyber Physical Systems

I Cyber Physical Systems (CPS) sono una delle innovazioni tecncologiche della quarta rivoluzione industriale.

Sono sistemi il cui meccanismo è monitorato da algoritmi computer-based. Le componenti fisiche e software sono fortemente interconnesse in modo tale da poter operare su diverse scale temporali e spaziali e poter interagire tra loro in modi differenti in base ai cambiamenti del contesto. L'insieme di queste tecnologie è in grado di dar vita ad un ulteriore sistema basato sull'integrazione tra vari soggetti, posti anche a distanza tra loro.

In essi si fondono conoscenze riguardanti la meccatronica, la cibernetica, il design e la scienza dei processi.

Livelli di funzionalità

Cinque livelli di funzionalità:

- Smart Connection: utilizzo di sensori per la gestione dei dati;
- Data-to-information-connection: aggregazione e conversione dei dati con aggiunta di eventuali informazioni;
- Digital Twin: sintetizzazione del dominio reale nella realtà digitale;
- Cogniction: considerazione di tutti gli scenari possibili. Indispensabile per un processo decisionale adeguato;
- Configuration: proiettare la realtà virtuale su quella fisica tramite l'invio di feedback.

Tecnologie

Tre tipologie di tecnologie abilitanti:

- Sensori integrati: ciascun sistema in pochi secondi riesce a capire la propria situazione operativa e inviare le informazioni relative al proprio stato e alla posizione;
- Attuatori: consentono lo svolgimento delle varie azioni senza rischi per rendere ogni processo più performante;
- Intelligenza decentrata: elabora gli scenari di scelta per fornire il più rapidamente possibile quello più consigliato.

L'insieme delle tecnologie costituisce il dominio digitale che permette alle informazioni di muoversi e garantisce una connessione veloce tra i componenti fisici.

Vantaggi

L'utilizzo dei Cyber Physical Systems può portare a:

- Nuove possibilità di business;
- Digitalizzazione del prodotto;
- Migliore gestione della produzione e delle performance;
- Gestione di impianti, macchinari e attrezzature più semplice;
- Trasferimento di informazioni e conoscenze più veloce.

Argomenti

Attacchi

Gli attacchi ai Cyber Physical Systems sono di tre tipi:

- **Attacchi all'availability del sistema**;
- **Attacchi all'integrità dei dati**: noti anche come *deception attacks*, rappresentano la classe più ampia di attacchi;
- **Attacchi alla riservatezza**: noti anche come *disclosure attacks*.

Principali attacchi

I principali attacchi che colpiscono i CPS sono:

- **False data injection**: appartengono ai *deception attacks* e riguardano la stima dello stato. É uno degli attacchi più studiati. L'avversario conosce le infromazioni topologiche del sistema e manipola le misurazioni dei sensori per modificare la variabili di stato, baypassando gli schemi di rilevamento dei dati errati.
- **Generic deception**: è un attacco all'integrità dei dati. L'avversario invia false informazioni a uno o più sensori o controllori in modo tale da ingannare un componente compromesso e fargli credere che il falso dato ricevuto sia valido. É modellato come un segnale additivo arbitrario, mandato a sovrascrivere i dati originali.

Principali attacchi

- **Denial of Service (DOS)**: è il più noto tra gli attacchi alla disponibilità. Rende inaccessibili alcuni o tutti i componenti di un sistema di controllo e impedisce la trasmissione dei sensori e del controllo sulla rete.
- **Replay**: fa parte degli attacchi all'integrità dei dati e solitamente viene combinato con un attacco fisico. L'avversario prima raccoglie sequenze di dati di misurazioni o controllo, poi riproduce i dati registrati mentre inietta un segnale esogeno nel sistema. Può non conoscere il modello del sistema per generare un output dannoso ma, conoscendolo, può raggiungere più facilmente il suo obiettivo, come per esempio danneggiare anche fisicamente l'impianto.

Principali attacchi

- **Covert misappropration**: l'avversario può ottenere il controllo dell'inpianto senza essere rilevato dal controllore. Questo attacco richiede alti livelli di conoscenza del sistema e l'abilità dell'avversario di leggere e sostituire i segnali di comunicazione all'interno dell'anello di controllo.
- **Zero dynamic**: l'avversario costruisce una *open-loop policy* in modo tale che il segnale d'attacco non produca output. Gli attacchi sono quindi disaccoppiati dall'uscita dell'impianto e risultano furtivi rispetto ai rilevatori di anomalie arbitrarie.

Caso di studio: dispositivi medici impiantabili

Argomenti

Difesa

Per difendersi dagli attacchi....