PROGETTO DI RICERCA

L'attività di ricerca sarà orientata a sostenere il programma previsto dai due progetti di Spoke 8 del PE 7 - SERICS, Ecocyber e Protect-IT. In entrambi i progetti, pur con caratteristiche diverse, sono previste attività focalizzate sull'identificazione di strumenti innovativi per garantire la protezione della comunicazione in rete, con particolare riferimento a specifici ambiti applicativi fra i quali spicca quello dell'industria manifatturiera.

Il progetto intende contribuire al WP2 del progetto Ecocyber, task 2 e ai WP 2 e 3 del progetto Protect-IT.

Il progetto parte dalla consapevolezza che è oggi possibile realizzare soluzioni aperte e omogenee per la raccolta di dati in ambienti manifatturieri (la cosiddetta Operation Technology o OT) sia dai componenti operativi, macchine ecc. sia dai componenti di rete, ad esempio utilizzando un componente chiamato Asset Administration Shell (AAS) che funge da rappresentazione digitale di un determinato asset. Queste soluzioni permettono di considerare la rete come parte del sistema OT, e quindi come un elemento attivo della gestione del processo produttivo.

Questo progetto intende esplorare in dettaglio la possibilità di utilizzare questo tipo di architetture software a supporto della sicurezza delle reti OT. In particolare si vuole indagare come integrare soluzioni di anomaly detection basate su tecniche di intelligenza artificiale con le rappresentazioni digitali degli asset di fabbrica al fine di monitorare i loro comportamenti in rete e reagire quanto più rapidamente possibile ad eventuali eventi inattesi, impostando un controllo a ciclo chiuso che combini qualunque situazione anomale identificata come un potenziale pericolo con l'attuazione di una relativa contromisura.

PIANO DI ATTIVITA'

Il piano di attività sui 12 mesi si articolerà in tre fasi.

1. Sperimentazione di AAS per componenti di rete.
2. Messa a punto di un sistema prototipale che arricchisca gli AAS con componenti basati su AI per l'analisi in tempo reale del traffico e l'identificazione di anomalie
3. Integrazione delle AAS con componenti di rete programmabili, capaci di modificare sulla base di semplici direttive il comportamento dei nodi di rete (utilizzando il linguaggio P4 per la programmazione degli switch)
4. Studio e sperimentazione di tecniche "closed loop" per combinare i risultati dell'analisi di monitoraggio con azioni attivi di contromisua contro eventuali attacchi alla sicurezza della rete OT.