



HAL
open science

Digital Twin and Intrusion Detection in a Cyber Physical System

Henry Chima Ukwuoma, Gilles Dusserre, Gouenou Coatrieux, Johanne Vincent

► **To cite this version:**

Henry Chima Ukwuoma, Gilles Dusserre, Gouenou Coatrieux, Johanne Vincent. Digital Twin and Intrusion Detection in a Cyber Physical System. Colloque IMT 2023: "Sécurité et Résilience", Apr 2023, Palaiseau, France. 2023, 10.5281/zenodo.7937270 . hal-04097871

HAL Id: hal-04097871

<https://imt-mines-ales.hal.science/hal-04097871v1>

Submitted on 15 May 2023

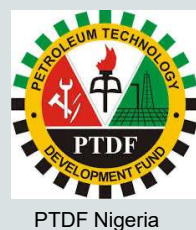
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Authors

Henry Chima UKWUOMA
Gilles DUSSERE
Gouenou COATRIEUX
Johanne VINCENT

Partners

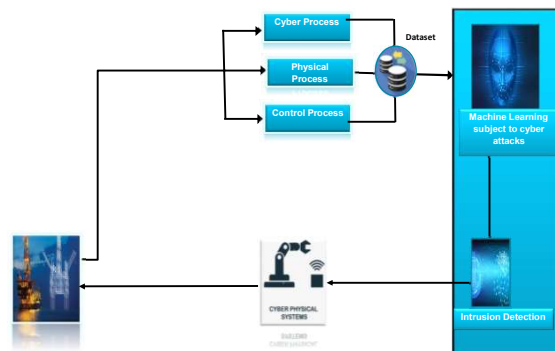


BACKGROUND

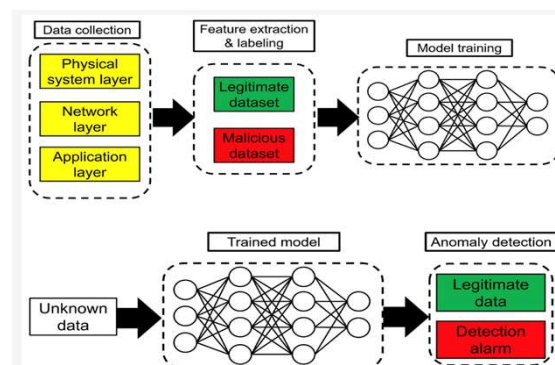
The security of Industrial Control Systems in the health sector represents a significant challenge in today's world. The occurrence of high-profile cyber security threats has penetrated the industries (health), mostly importantly with the advent of COVID-19.

Need to detect and prevent intrusions in a Cyber Physical System using machine learning via a replica (digital twin) for hospitals.

- **Digital Twin:** Digital twin is a virtual representation created to represent a real-world object such as a water management system. This study adopts a DHALSIM testbed
- **Cyber Physical System:** A system that consists of the coordination and combination of computational and physical components. The study adopts a water distribution network as a case study.
- **Intrusion Detection:** A tool or software program that monitors malicious activities or rule violations in a system.
- **Machine Learning:** Application of machine learning to a water management dataset for enhanced performance on a given set of tasks



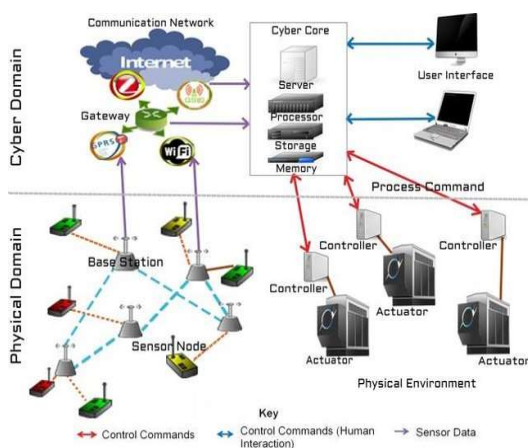
Conceptual Process Flow between the Digital Twin, Machine Learning Model for Intrusion Detection and the Cyber Physical System



Cyber-Physical Intrusions Detections system
Source: Kim and Park, 2021

RESEARCH OBJECTIVES

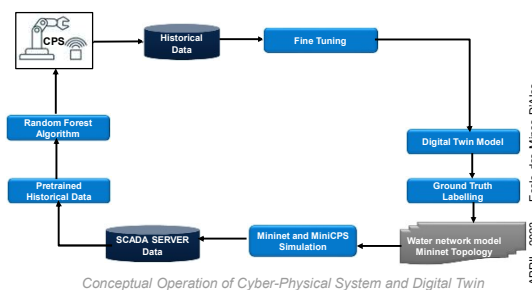
- To examine existing machine learning models deployed for cyber security in a water management system with the intention of designing an Intrusion Detection model for securing data in a Cyber Physical System (CPS).
- To establish if the machine learning models used for Intrusion Detection in CPSs can guarantee data security in respect to an enhanced cyber security for a hospital management system.
- To evaluate and validate the proposed model.
- To improve crisis management through simulation (Tabletop Exercises). How a Hospital Management System could anticipate, react and manage a hospital water system, in times a system is hijacked for malicious intentions.



Cyber-physical system architecture
Source: Ledwaba and Venter, 2017

EXPECTED RESEARCH OUTCOMES

- **Behavioural analysis** of the CPS with and without cyber attacks via the Digital Twin.
- **A machine learning model** for the detection of intrusions in a Cyber Physical System via a digital Twin (DHALSIM testbed)
- **Ways and means to manage** a water distribution systems during cyber attacks



Conceptual Operation of Cyber-Physical System and Digital Twin