SIGA Level Zero OT Resilience

Extension Project Proposal

SIGA at ICRDE

- 2 independent work packages
- False-Data-Injection (FDI) attack detection
- Closely aligned with our ongoing collaboration with ASU

SIGA Level Zero OT Resilience

Advanced Collaboration with ASU for Simulated Attack Generation

SIGA Level Zero OT Resilience

Objective

- Simulate advanced attacks from the adversary's perspective, with the primary goal of minimizing or evading detection by SIGA's system while ensuring system model and Bad Data Detection (BDD) consistency
- Enhance SIGA's models' layer to bolster its detection capabilities and address the challenges above

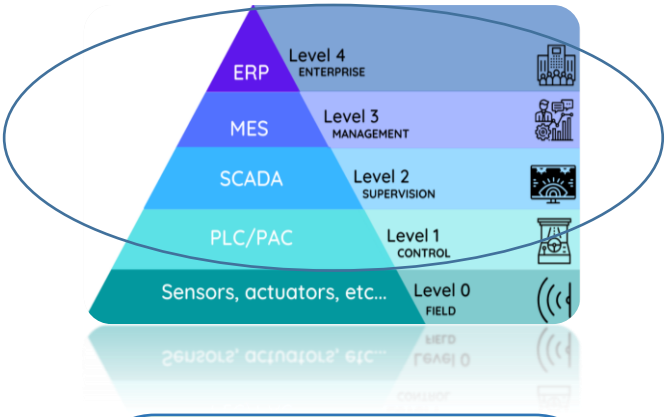
SIGA at ICRDE

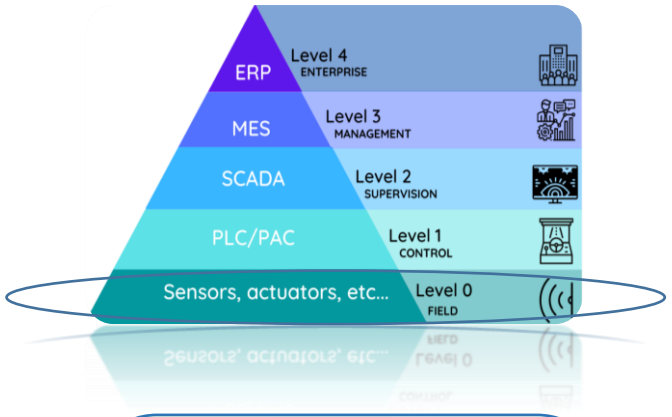
SIGA Level Zero OT Resilience

Optimization of SIGA's detection based on inter-level monitoring

SIGA at ICRDE

SIGA Level Zero OT Resilience





- Unsupervised anomaly detection
- Time-series data
- Process-oriented context

Optimized subset selection

Advanced validation of measurement's consistency

- Physical layer (level 0)

Vs.

- Reported values (levels 1-3)

Ultimate effectiveness against False-Data-Injection cyber attack

SIGA Level Zero OT Resilience

Objective

Optimizing the selection of a given set of IOs:

Given an accumulated dataset representing their inter-correlations and a target subset size of X%, we aim to identify the subset that minimizes the ability to execute FID cyber-attacks on the remaining (100-X)% of IOs without detection