SIGAGUARD

Cyber Resiliency Solution for Data Centers

A paradigm shift for organizations with ZERO TOLERANCE for operational downtime, due to process disruption, in-efficiencies or failure of critical assets. Whether caused by Cyber Attacks, Malfunctions, Misconfigurations or a Human Error, SigaGuard detects process anomalies from Level 0 (the process level) to ensure operators act upon on these threats quickly and efficiently.

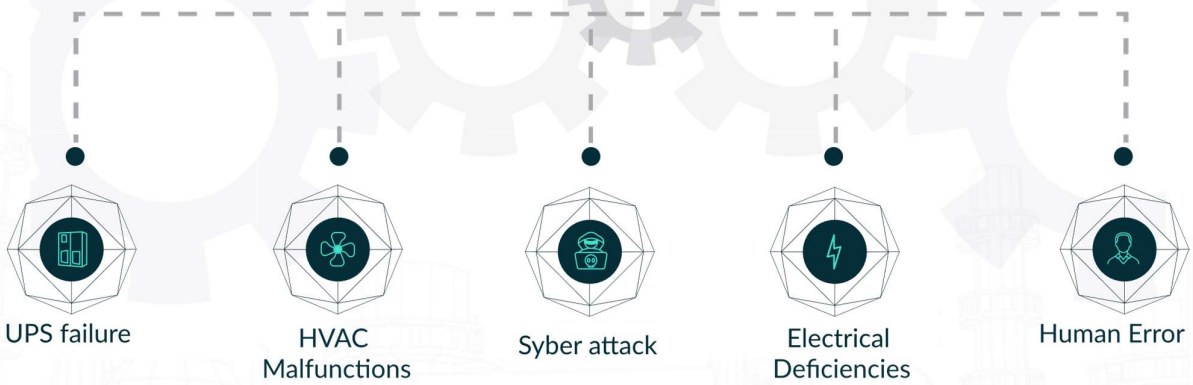
While securing the data-network is crucial, the system's process level is left unmonitored, leaving the system highly vulnerable despite the network layers of protection in place. Severe threats can go unnoticed by operators as demonstrated in past events such as : Stuxnet (2010), Irongate (2016), and Black Hat (2019) where PLCs were compromised by hackers without the network-solutions' detection or the operators' awareness of such event.

This vulnerability can be solved by monitoring the most reliable source of information, the raw electrical signals at level 0 – sensors and actuators, connected to the mission-critical assets (generators, UPS, air-conditioning systems, electrical rooms etc).

A data center's main function is to provide constant uptime for the mission-critical applications it houses.
Any downtime in a Data Center negatively affects your business.

Every minute of downtime costs a data center an estimated cost of 8,000$ According to Forbes, ransomware attacks during 2021 caused organizationsa 20 $ billion loss. This disturbing figure is expected to grow, costing organizations 265 billion dollars by 2031

The top causes for Unplanned Downtime in Data-Centers



SigaGuard safeguards data center assets by using an out-of-band network to monitor raw, untampered electrical signals. These signals are analyzed by SIGA's unsupervised machine learning software to provide operators real-time alerts on anomalies or operational failure indicators to maximize uptime.