SIGA Level Zero OT Resilience

Task Goal

Novel early warning detection capabilities for a power grid with geographically dispersed assets will be developed, based on the latest ML technology developed by SIGA with expanded process monitoring capabilities.

SigaGuard Current 1-to-1 Architecture

Monitoring and anomaly detection on a single asset object

SIGAGUARD

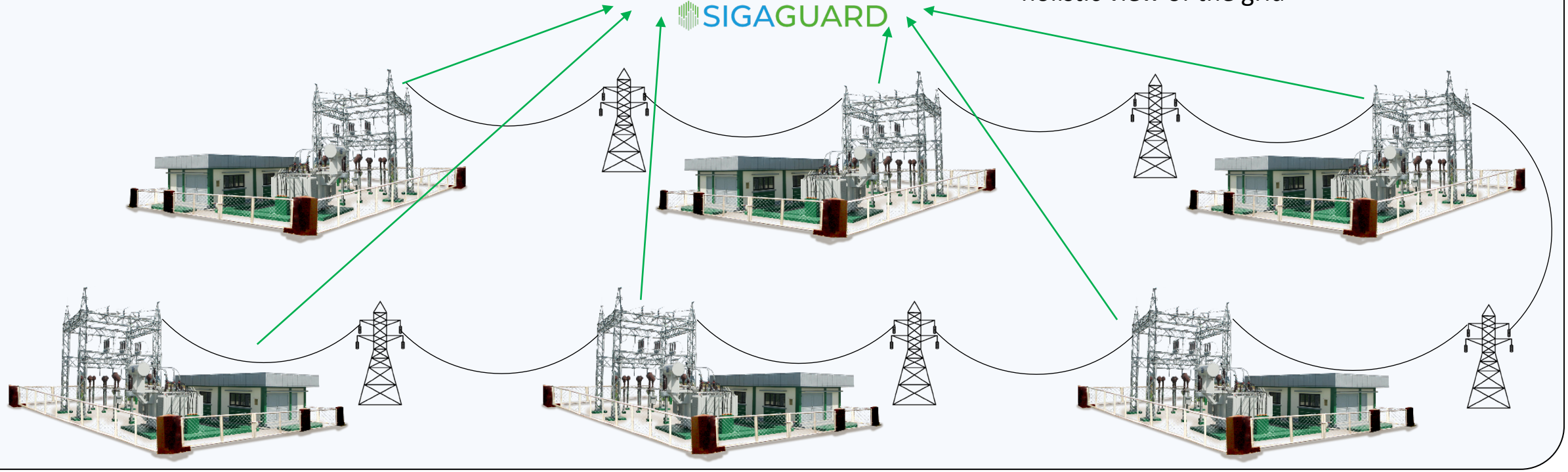
- Monitor and analyze each specific site as one, without correlation with other sites.
- Independent visualization and dashboard for each site

SigaGuard Developed Many-to-1 Architecture

Monitoring and anomaly detection on a multiple-assets object (for power grids)

SIGAGUARD

- Monitor and analyze multiple geographically dispersed energy distribution sites as one object, deriving high level conclusions from the distributed sites' alerts and data
- Centralized visualization and dashboard for a holistic view of the grid



SIGA at ICRDE – Task 9

SIGA Level Zero OT Resilience

Path for new tool development

S3
- Framework for multiple sites data collection and processing.

S4
- Fully designed novel detection approach to use algorithms on a larger (x10) scope of data
- New approach validity tests

S5
- Fully ready algorithmic and framework implementation for x10 data scope
- New detection algorithm for multiple sites' processes and sensor data
- Dashboard for centralized visualization and monitoring of all sites

S6
- New Tool in full production ready state
- Tools installed and tested on partners' sites or testbeds

Collaboration with other partners

Data Providers for Development?

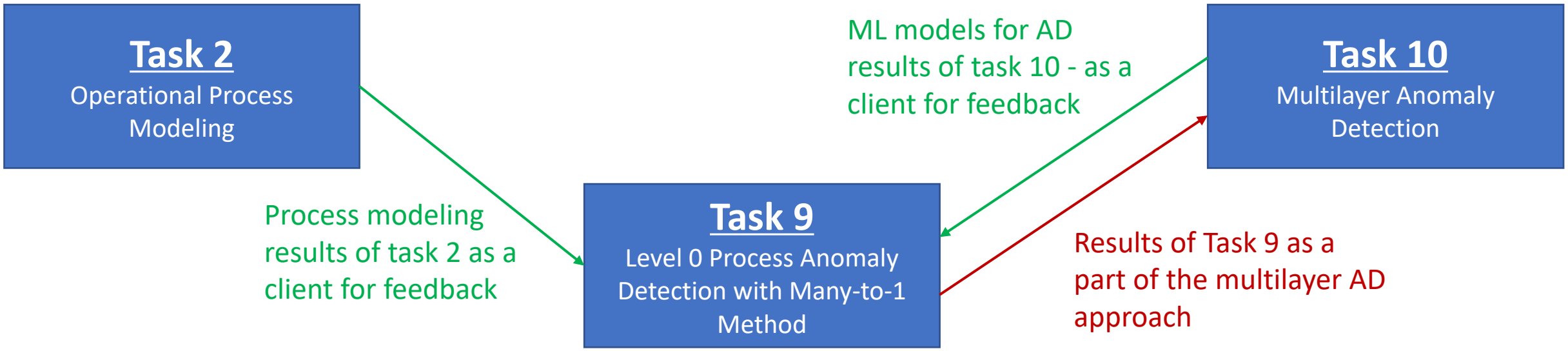
Planned Development: SIGA Many-to-1 Architecture

Use Cases Pilots?

Research Cooperation:

SIGA Level Zero OT Resilience

Integration with other tasks



Potential Impact

- Level 0 of the OT is an important layer to monitor and secure as a part of a multi-layer security approach
- The transformation from 1-to-1 to Many-to-1 will enable monitoring at level 0 of multiple assets as one asset. (i.e., monitoring a whole power grid as one asset and not only for single substations as a group of assets)
- The results above will bring to better resilience of the OT systems and processes in the power grid