SIGA
Level Zero OT Resilience

New York Power Authority

Energy Sector Use Case NYPA

Elevating OT cybersecurity to Level 0

The client

New York Power Authority (NYPA)

The New York Power Authority is the nation's largest state public power organization, with 16 generating facilities and more than 1,400 circuit-miles of transmission lines.

Elevating OT cybersecurity to Level 0

SIGA
Level Zero OT Resilience

New York Power Authority

The challenge

- SIGA monitors a 345 kV NYPA Substation in a lab environment.
- The monitored substation includes:
  - 2 capacitors status
  - Bus voltage measurement
  - Current measurements
  - STATCOM device

SIGA
Level Zero OT Resilience

The process

1) SIGA system was installed.
2) SIGA learned the normal behavior of the sub-station operation for 2 weeks.
3) The asset owners performed a cyber-attack on the process SCADA's RTU, by simulating 4 different attack scenarios in 1 hour.
4) SIGA detected the anomalies in real-time of all cyber-attacks that were initiated and alerted the operators.

The solution

SigaGuard provides ultimate granular process visibility delivering the most reliable insights coming directly from the electrical signals at Level 0.

By reporting to the engineers of malfunctions to the process in real-time, downtimes can be reduced to a minimum and even be prevented.

SigaGuard is an out-of-band solution which ensures that the operators can feel the machinery's pulse and act upon the threats quickly and efficiently to protect and improve critical processes.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #1 – RTAC REBOOT ATTACK

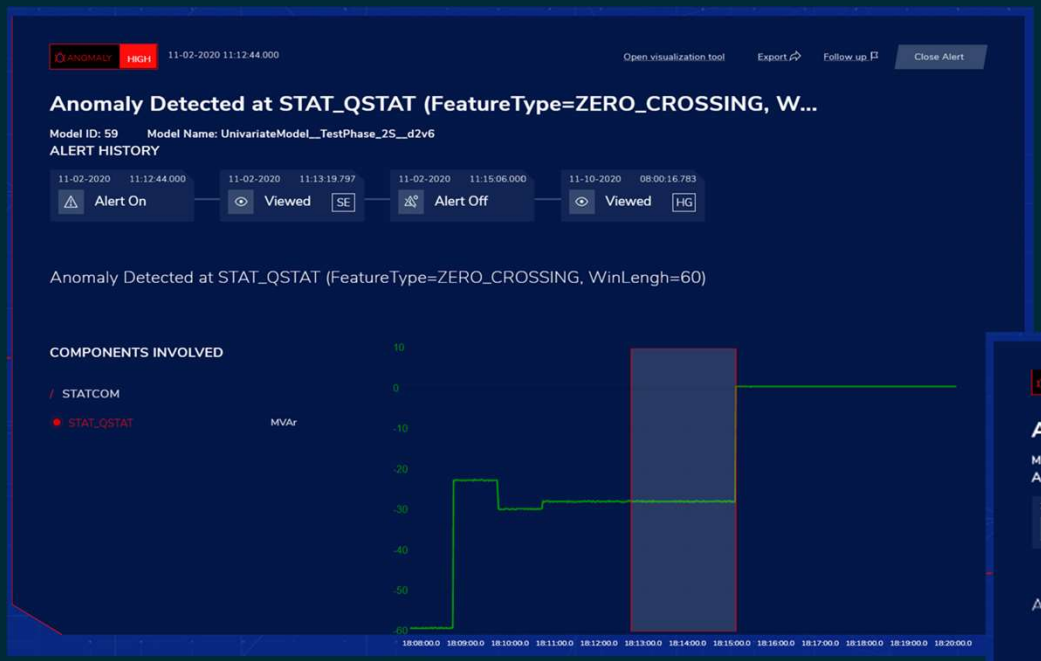
Misbehavior: RTAC Rebooted
Result: "STAT_QSTAT" setpoint is not being re-calculated as expected

Misbehavior: Voltage rapid disturbance simulated
Result: "MARCY_V_RMS" voltage is peaking up and down

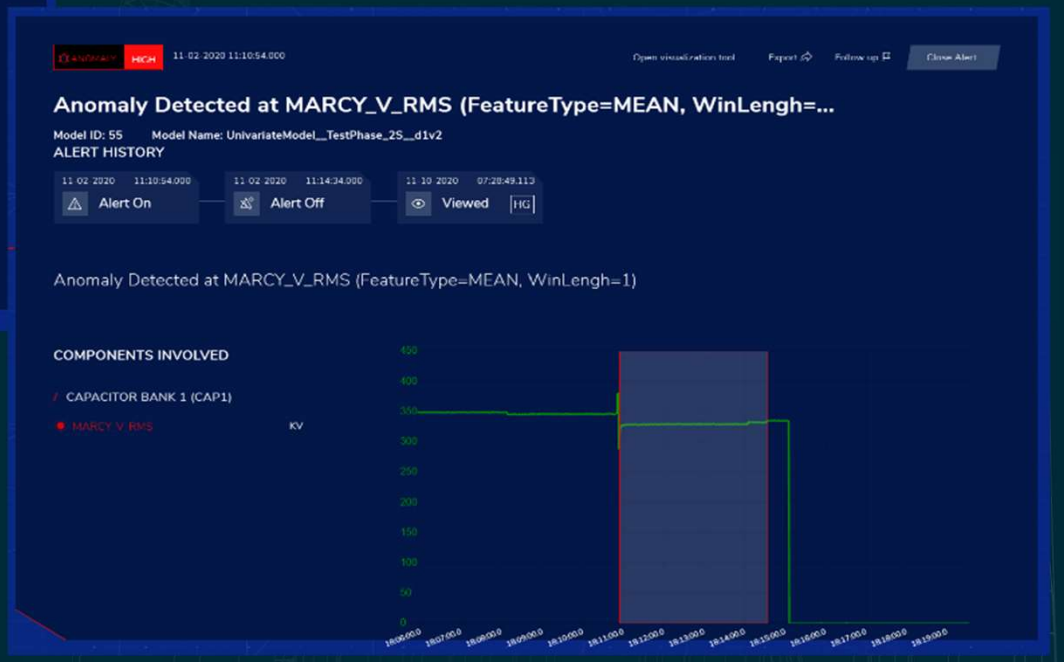
SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #1 – SIGA DETECTION



Alerts displayed in SIGA's dashboard

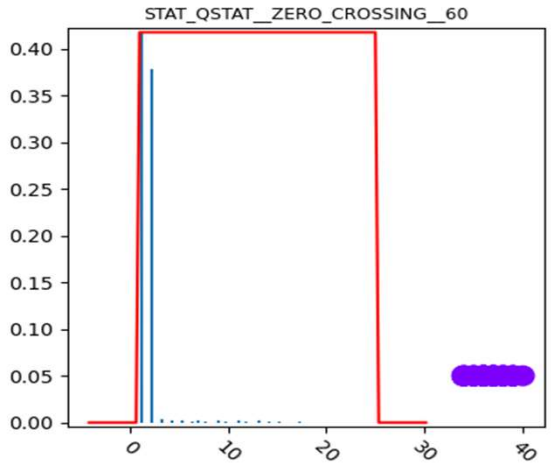


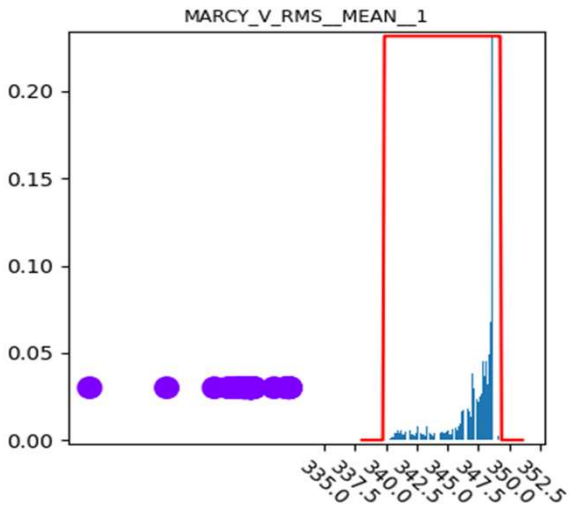
SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #1 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool





SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #2 – INVALID COMMAND TO CAPACITORS

Misbehavior: When voltage rises, the capacitor is turned ON instead of staying OFF
Result: "CAP1_BRK_CTRL" is ON, "MARCY_V_RMS" stays too high

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #2 – SIGA DETECTION

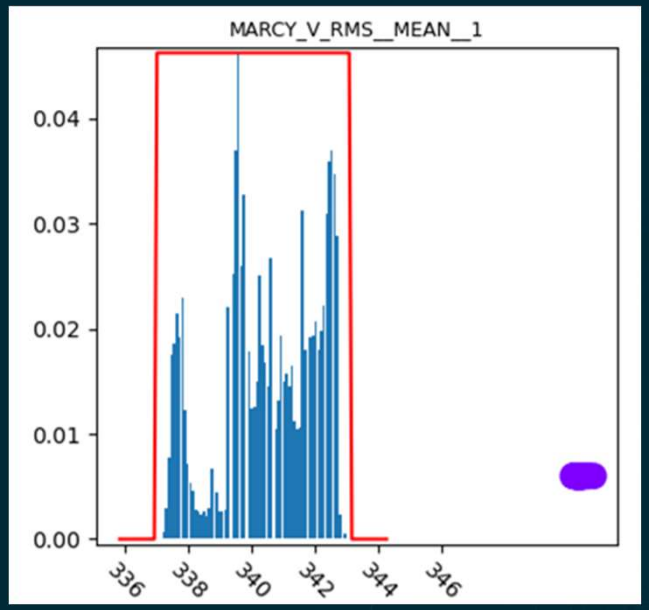
Alerts displayed in SIGA's dashboard

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #2 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



ML Model is analyzing the IOs behavior in the state: [CAP1=1, CAP2=0]

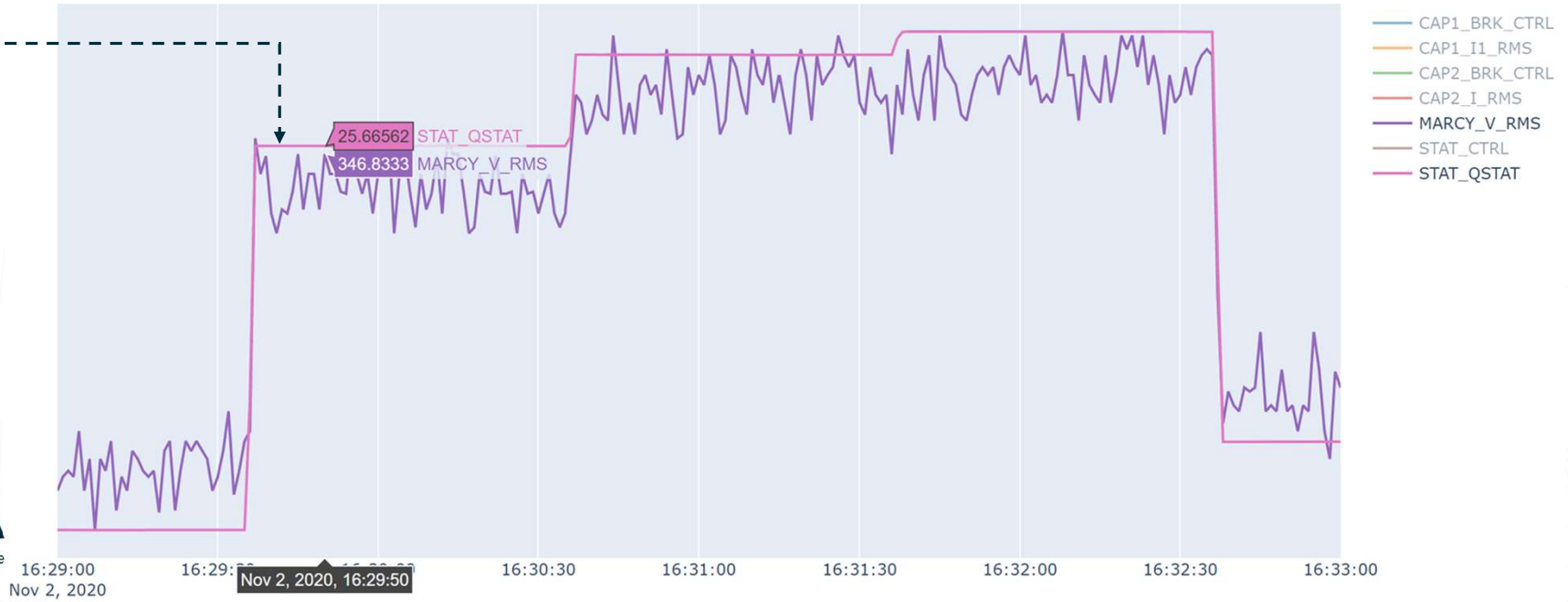
SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #3 – INVALID COMMAND TO STATCOM – SETPOINT IS INCREASED BY 20%

Misbehavior: "STAT_QSTAT" setpoint is produced by RTAC with a 20% deviation from the expected calculated setpoint

Result: Miscorrelation between "STAT_QSTAT" and "MARCY_V_RMS"



SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #3 – SIGA DETECTION

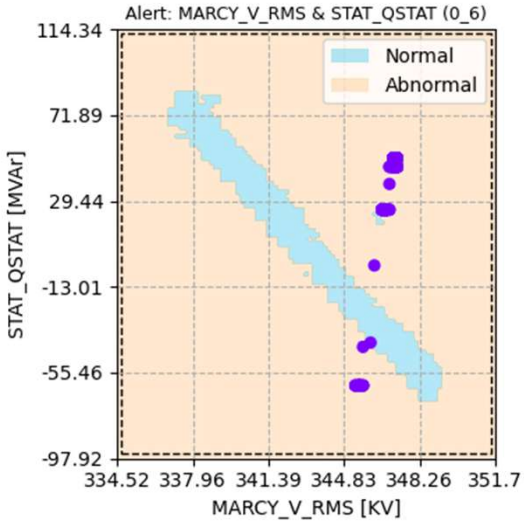
Alerts displayed in SIGA's dashboard

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #3 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



ML Model is analyzing the

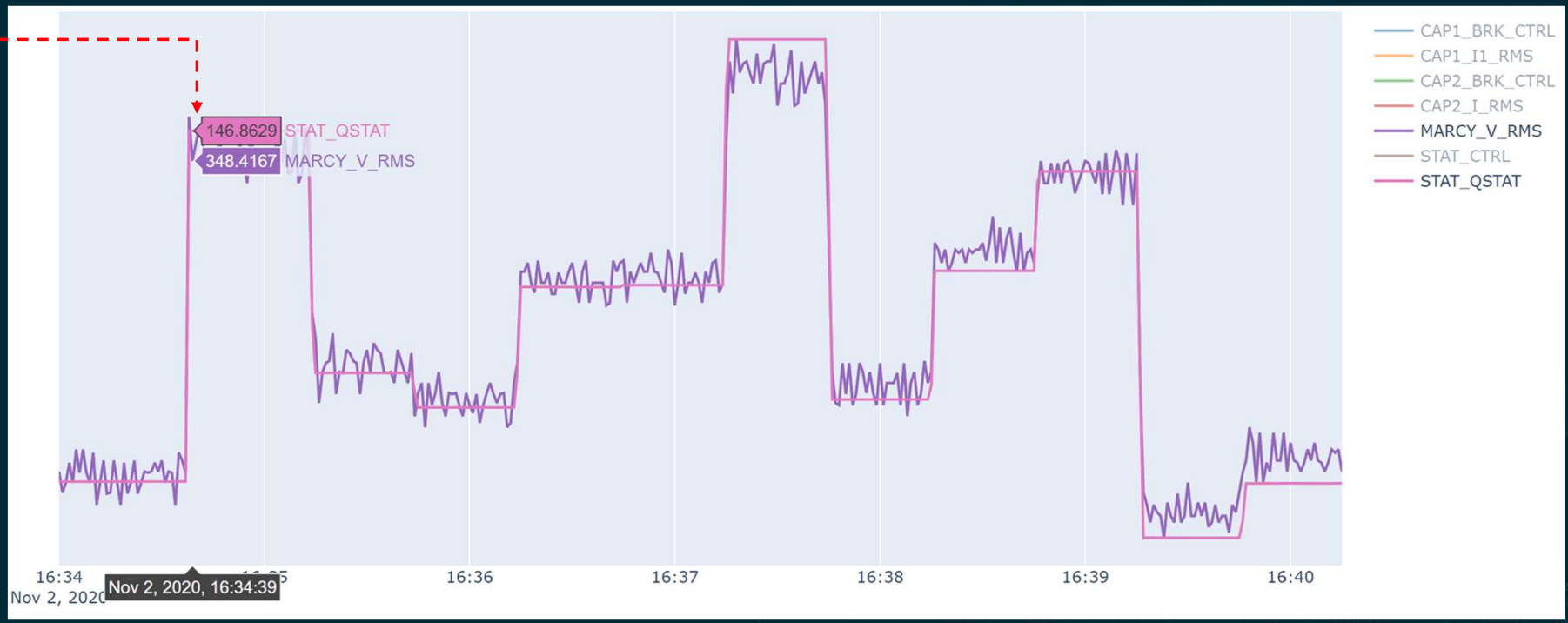
IOs correlation

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #4 – INVALID COMMAND TO STATCOM – SETPOINT IS RANDOM

Misbehavior: *"STAT_QSTAT" setpoint is produced by RTAC with a random value*
Result: *Miscorrelation between "STAT_QSTAT" and "MARCY_V_RMS"*



SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #4 – SIGA DETECTION

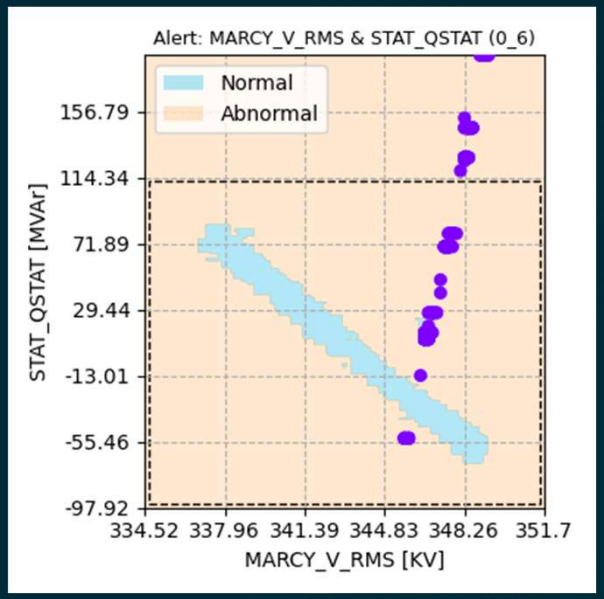
Alerts displayed in SIGA's dashboard

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

ATTACK #4 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



ML Model is analyzing the

IOs correlation

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

SigaGuard unparalleled offering

The most advanced solution for detecting and analyzing cyber-attacks on mission-critical automated equipment, machinery and processes.

Reduces downtime to a minimum: Unmatched visibility ensures a quick and safe recovery from downtimes.

Inaccessible insights: SigaGuard delivers precise granular visibility with cutting-edge AI insights.

Feeling the machinery's pulse: SigaGuard provides operators with the most reliable source of data

Data archives: Improved preparedness for future attacks

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

Conclusion

- The attacks were chosen by NYPA, focusing on the main cyber scenarios affecting the operation of the sub-station with either false or no reporting to the control level.
- In these types of attacks, once perimeter is breached, the process is exposed to the attackers' manipulation while being masked from the control.
- SigaGuard has detected all four attacks, all in less than 1 second from the attack.
- All attacks were identified by multiple models, setting high probability of cyberattack.
- SIGA has demonstrated its unique advantages in this set of tests as a complete detection success.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

About SIGA

Founded in 2014, SIGA OT Solutions is an innovative cybersecurity company driving a paradigm shift within the world of OT cybersecurity. The company strives to expand the boundaries of OT operations with deepened security and elevated process integrity, by delivering AI enhanced monitoring and deeper operational perception to operators of critical assets.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0