



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.





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







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 <u>out-of-band solution</u> 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.



ATTACK #1 – RTAC REBOOT ATTACK



ATTACK #1 – SIGA DETECTION

International producted at STAT_QSTAT (FeatureType=ZERO_CROSSING, W Model 1D: 59 Model Name: UnivariateModel_TestPhase_2S_d2v6 Alert HISTORY International producted at STAT_QSTAT (FeatureType=ZERO_CROSSING, WinLengh=60)	Alerts displayed in SIGA's dashboard
COMPONENTS INVOLVED 10	
/ STATCOM	11-02-2020 11:10:54:000 Dpen visualization tool Export 🏟 Entre up 🛛 Classe Allert
STATLOSTAT MVAr .10	Anomaly Detected at MARCY_V_RMS (FeatureType=MEAN, WinLengh=
	Model ID: 55 Model Name: UnivariateModel_TestPhase_2S_d1v2 ALERT HISTORY
-50	11 02 2020 11:10:54:000 11 02 2020 11:14:34:000 11 10 2020 07:20:49:113 ▲ Alert On ▲ ▲ Alert Off ④ Viewed HG
	Anomaly Detected at MARCY_V_RMS (Feature lype=MEAN, WinLengh=1)
1800000 1810000 1810000 1810000 1812000 1812000 1812000 1815000 1815000 1815000 1815000 1815000 1819000 1820000	
	COMPONENTS INVOLVED 400
	/ CAPACITOR BANK 1 (CAP1)
	300 JUNE 10 JUNE 100
SIGA	
Level Zero OT Resilience	bookar bookar bootan bastan

ATTACK #1 - SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



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



ATTACK #2 - SIGA DETECTION

Model ID: 54 Model Name: UnivariateModel_ ALERT HISTORY	TestPhase_2Sd1v1		
11-02-2020 11:23:18.000 11-02-2020 11:2 Alert On	7:14.000 11-12-2020 00:21:46.597 Viewed HG		
Anomaly Detected at MARCY_V_R	MS (FeatureType=MEAN, WinLengh	=5)	
COMPONENTS INVOLVED			
/ CAPACITOR BANK 1 (CAP1)			
			11

SIGA

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]

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



ATTACK #3 – SIGA DETECTION

Todel 10: 53 Model Name: TreesCorrelationM ALERT HISTORY 11-02-2020 11:30:38.000 11-02-2020 11:3	dellestPhase_2Sd1v2				
11-02-2020 11:30:38:000 11-02-2020 11:3					
▲ Alert On 🛛 💿 Viewed	20.893 11-02-2020 11:32:36.000 SE A ^o Alert Off	0 11-11-2020 04:47:13.850			
APCY V PMS and STAT OSTAT	are out of correlation (state	a-0)			
COMPONENTS INVOLVED			-		
CAPACITOR BANK 1 (CAP1)					
I MARCY_V_RMS KV 🗠					
STATCOM					
STAT_QSTAT MVAr	350 - Michannelly works	my man man	www.www.w	~	



Alerts displayed in SIGA's dashboard

ATTACK #3 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



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"



ATTACK #4 – SIGA DETECTION

ALERT HISTORY			
11-02-2020 11:34:40:000 11-02-2020 11:35:16.0 ▲ Alert On & Alert Off	00 11-11-2020 07.09.59.647		
MARCY_V_RMS and STAT_QSTAT are	out of correlation (state=0)		
COMPONENTS INVOLVED			
/ CAPACITOR BANK 1 (CAP1)			
e Marcy_v_rms 🛛 🛛 🗸			
/ STATCOM			
• STAT_QSTAT MVAr 💽	350 Ad-5 talk and recover and any other		and the second

SIGA

ATTACK #4 – SIGA DETECTION

Alerts displayed in SIGA's ML visualization tool



ML Model is analyzing the

IOs correlation

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



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.









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.