Superior Performance by SigaGuard at CISS2019 Showdown

The Critical Infrastructure Security Showdown (CISS) 2019

In August 2019, SIGA participated at the Critical Infrastructure Security Showdown (CISS) 2019 in Singapore, partnering with ST Engineering, alongside global leading Cyber OT solution providers.

The full report was recently published, and is now fully available. The results show that SigaGuard (as part of Product D) received highest ranking score for detection of cyber-attack anomalies related to the OT process. The results explicitly demonstrate, beyond any doubt, that monitoring the electrical signals at level 0 is a crucial element for any cybersecurity protection platform in industrial environments.

Background

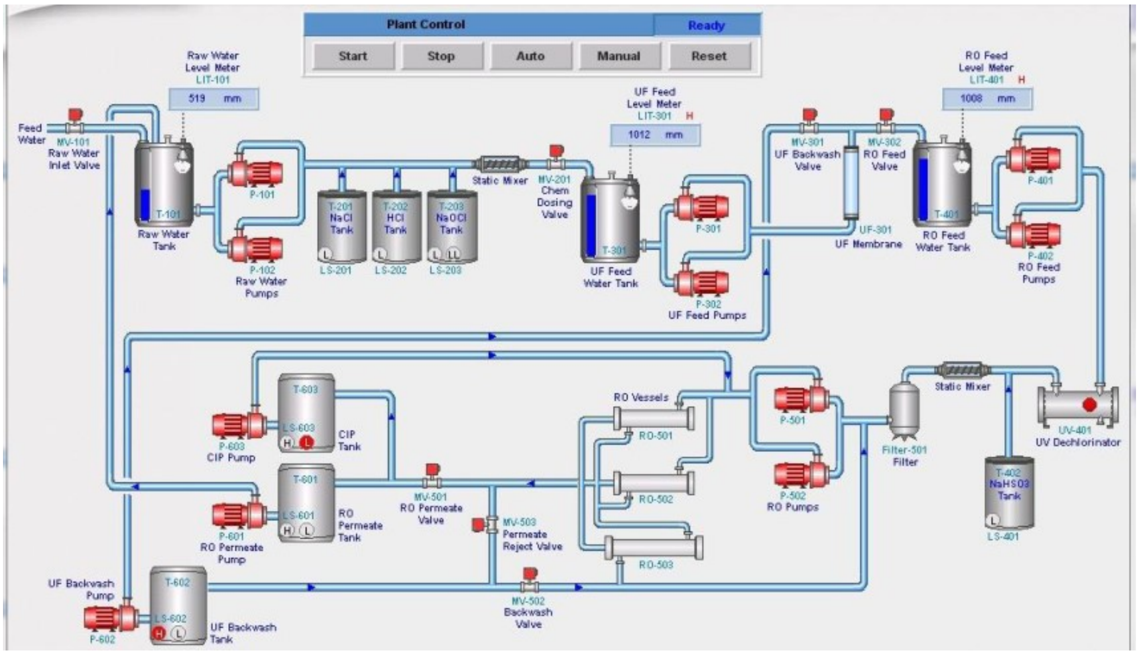
The Critical Infrastructure Security Showdown (CISS) 2019 is the third run of iTrust's technology assessment exercise. Organized by iTrust, the CISS 2019 exercise took place at SUTD (The Singapore University of Technology and Design) from the 26th to the 30th of August, 2019, and involved seven Red Teams and ten Blue Teams from both academia and leading Cyber OT players from the industry. The testbed consisted of a modern six-stage water treatment process that closely mimics a real-world treatment plant. Among the objectives of the exercise was to enable blue teams to showcase their detection capabilities against cyber-attacks.

The Process

Stage 1 of the physical process begins by taking in raw water, followed by chemical dosing (Stage 2), filtering it through an Ultrafiltration (UF) system (Stage 3), dechlorination using UV lamps (Stage 4), and then feeding it to a Reverse Osmosis (RO) system (Stage 5). A backwash process (Stage 6) cleans the membranes in UF using the RO permeate.

The testbed water treatment plant

The network and cyber portion of SWaT consisted of a layered communications network, Allen-Bradley Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) workstation, and a Historian. Data from sensors is available to the SCADA system and recorded by the Historian for subsequent analysis.



HMI/SCADA screenshot

SIGA's Level 0 Monitoring and Anomaly Detection

SIGA activated the **SigaGuard** solution for level 0 monitoring by listening to the electrical signals of the water treatment process, gaining direct visibility into the OT process. The integration was made into 18 analog I/O's as depicted below and provided an isolated out-of-band monitoring environment which cannot be manipulated or circumvented by the network level, therefore, reflecting the exact behavior of the critical asset being protected against any cyber-attack.

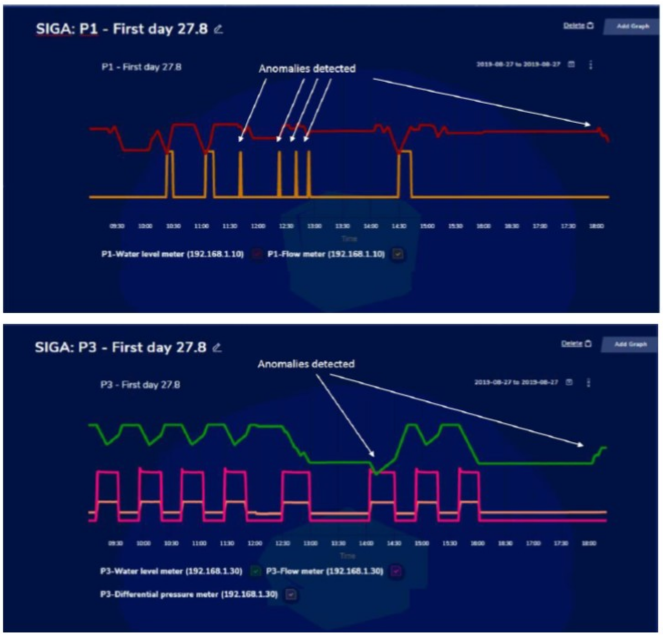
No.	Type (A/D/I/O)	DESCIPTION
0	A	Water level meter
1	A	Flow meter
2	A	Conductivity meter
3	A	PH meter
4	A	ORP meter
5	A	Water level meter
6	A	Flow meter
7	A	Differential pressure meter
8	A	Water level meter
9	A	Flow meter
10	A	PH meter
11	A	ORP meter
12	A	Conductivity meter
13	A	Inlet flow meter
14	A	Flow meter
15	A	Flow meter
16	A	Pressure meter
17	A	Pressure meter

SIGA's I/O Table

Results

More than 90% of documented successful attacks were level 0 attacks (i.e. attackers' objective was manipulation of the actual OT Level 0 process). See more information in the appendix below. This demonstrates again that in OT environments, the attackers ultimate objective will always be to reach down to the physical process (level 0) and affect it.

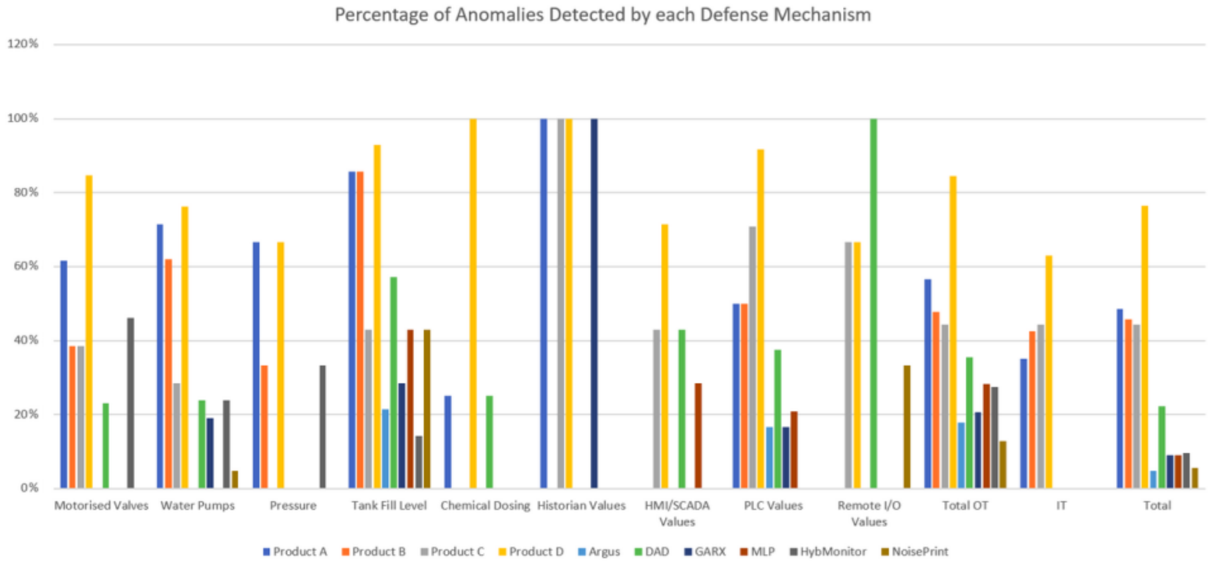
The results show that 85% of total OT anomalies were detected by **Product D** (while the next runner up succeeded detecting only 57%). In total, 54 physical process anomalies were recorded. With respect to sensor data anomalies, *"Product D performed significantly better than all other technologies;… Product D detected 30 out of 35 attacks i.e., about 85% of the attacks."*


SIGA: P1 - First day 27.8
Delete
Add Graph
P1 - First day 27.8
Anomalies detected
2019-08-27 to 2019-08-27
P1-Water level meter (192.168.1.10)
P1-Flow meter (192.168.1.10)
SIGA: P3 - First day 27.8
Delete
Add Graph
Anomalies detected
P3 - First day 27.8
2019-08-27 to 2019-08-27
P3-Water level meter (192.168.1.30)
P3-Flow meter (192.168.1.30)
P3-Differential pressure meter (192.168.1.30)

SIGA's anomaly detection screen shots during the CISS Showdown

As seen in the graph below: "*Across the commercial products, Product D outperformed the other products. It had a 100% detection rate for (e) and superior detection rates for attacks (a) to (d).*"

In other words, the combination of level 0 monitoring (SigaGuard) is critical in Cybersecurity platforms, outperforming any other tool, where detection of real-time cyber-attacks on critical OT processes is needed.



Product D outscored in all fields!

Summary of the published successful attacks:

1. DB attack – changing values in the database.
   Not a level 0 attack (no process affects). Would have been detected by PRS.
2. Water pump control – sending false commands to the PLC.
   A level 0 attack.
3. Valve control – sending false commands to the PLC.
   A level 0 attack.
4. Changing process operation resulting with damage of the system (not carried out to prevent damage).
   A level 0 attack.
5. Complex process manipulation – sending false commands to the PLC.
   A level 0 attack.
6. DDoS attack on the historian
   Pure network attack, no level 0 affects.
7. Raw Water System valves, including control of chemical dosing.
   A level 0 attack.
8. Raw Water System pump – sending false commands to the PLC.
   A level 0 attack.
9. Raw Water tank control – direct attack on the PLC.
   A level 0 attack.
10. Water pumps control – sending false commands to the PLC.
    A level 0 attack.
11. Valve control – sending false commands to the PLC.
    A level 0 attack.
12. Modifying process control – modifying control params on the PLC.
    A level 0 attack.
13. Plant shutdown – shutting down the plant by taking control of the HMI.
    A level 0 attack.
14. Modifying valves and pumps including changing PLC set point.
    A level 0 attack.
15. HMI-PLC communication attack – changing values sent from the PLC to the HMI.
    Not a level 0 attack (no process affects). Would have been detected by PRS.
16. Modifying values sent from remote sensors to the PLC affecting the process.
    A level 0 attack.
17. Plant control (start and stop) – taking control of the HMI.
    A level 0 attack.
18. Water pump control.
    A level 0 attack.
19. Pressure control via valve and pump.
    A level 0 attack.
20. Valve control – changing values sent between PLCs.
    A level 0 attack.
21. Water pumps control.
    A level 0 attack.
22. Manipulating chemical dosing and mixture via pumps control.
    A level 0 attack.
23. Stuxnet type attack – activating UF feed pump while transmitting it's off.
    A level 0 attack + extra value could have been added via PRS.
24. Raw water pump manipulation – changing values sent between PLCs.
    A level 0 attack.
25. Full HMI control.
    A level 0 attack.