SIGAGUARD

PRM

Product Sheet

Parallel Reference Monitoring

HMI's Can be Fooled!

Detect anomalies before they damage your critical assets. SIGA's Parallel Reference Monitor (PRM) provides multi-level real-time monitoring, revealing otherwise undetectable Level-0 attacks

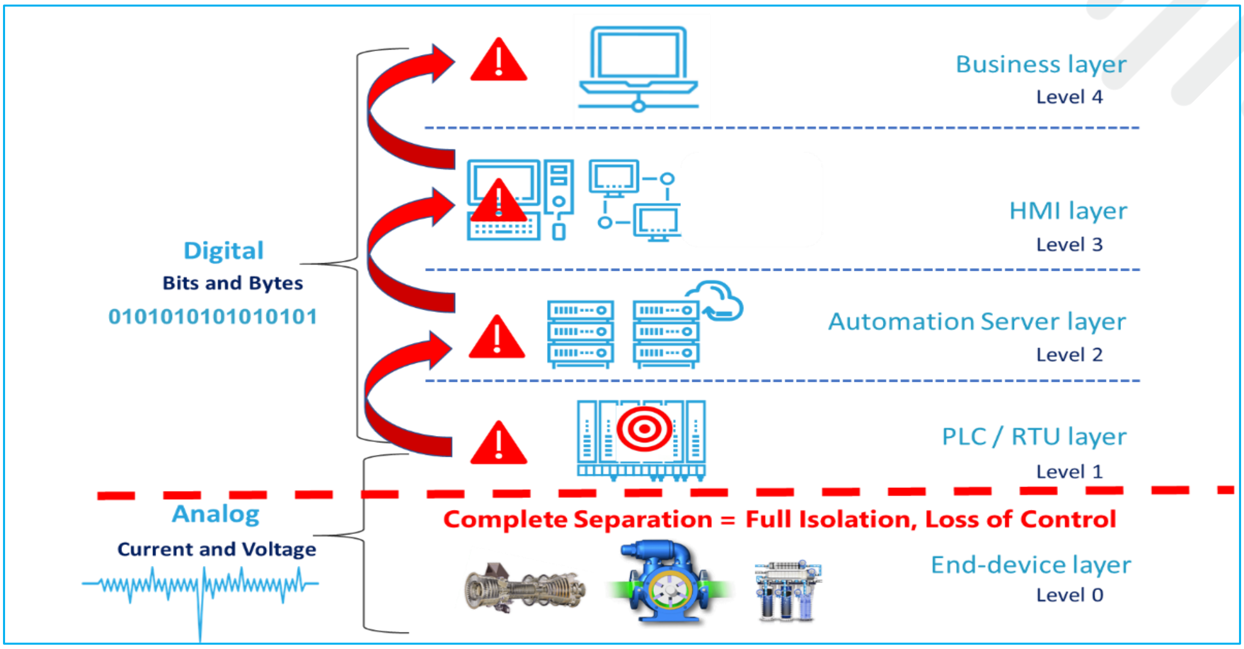
BACKGROUND

Existing SCADA environments are increasingly connected (IoT/IIOT) and as a result suffer from particularly high limitations in the ability to apply even the most basic security techniques, which are common in IT environments. Current security methods for industrial control systems are beginning to evolve and include network-level security, some use of firewalls, unidirectional diodes and protected gateways. Nonetheless, all of these security measures, that are designed to try and prevent unauthorized access via the Internet, enhance the severe level of threats to the SCADA environments, which are in many cases strategic objectives. This vulnerability and common operational constraints lead to very limited solutions, at best. Therefore, the SCADA's controller level, or Level 1 as it is called in the Purdue Model (e.g. PLC, RTU, etc.) can be compromised in various scenarios.

UNCOVERING STUXNET SCENARIOS

One of these dangerous scenarios (as illustrated in the figure below) is when an attacker takes control of a critical process while maintaining a perfectly proper operational appearance on all of the above monitoring tools (e.g. HMI). Moreover, the attacker will maintain this control without any detection capability by the control system operators. The control system's level 1, and therefore the upper levels as well, will be basically "blind" to the process that happens in Level 0 (the physical layer) and the attacker can damage assets without any knowledge of the process Operators and the upper layers.

AUTONOMOUS · RELIABLE · SMART



An attacker has taken control of a critical process while a perfectly normal operational status is reflected on the HMI and other levels. The attack is allowed to continue undetected because the control system's Level 1 (and above) monitoring devices are blind to what is happening at Level 0 (the physical layer).

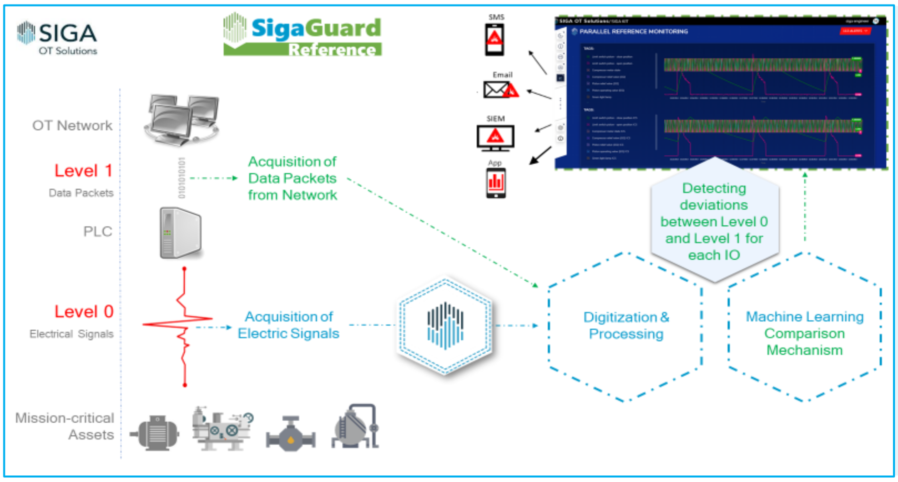
THE SOLUTION: PRM

SIGA's Parallel Reference Monitoring (PRM) product augments SIGA's critical process monitoring solution by comparing on one screen what operators are seeing at the HMI and other layers with what's actually happening at the end-device layer — and alerting the operators to any discrepancies..

Any inconsistency between the Level-0 status and that of the network levels is a red flag that a hacker may be spoofing the HMI and that an attack is already underway—unbeknownst to the operator.

How does PRM Work?

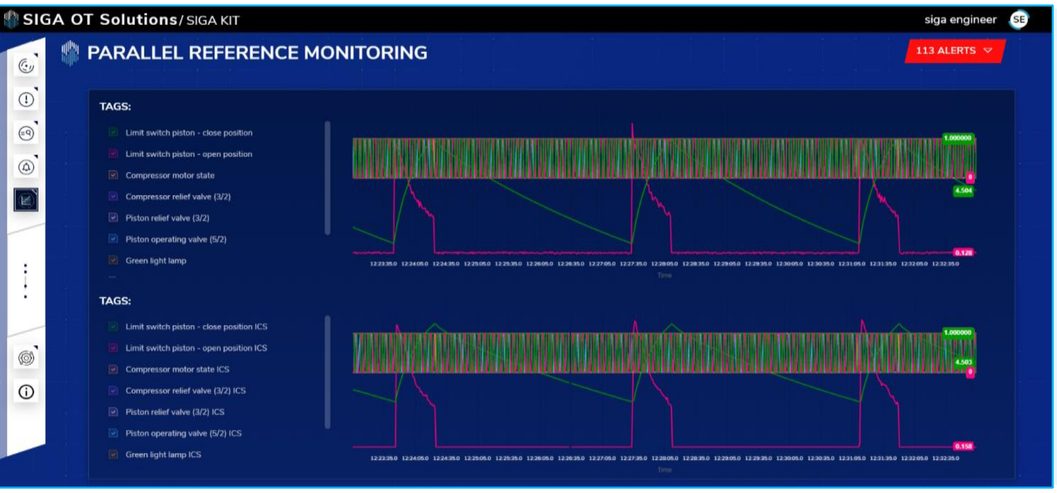
SIGA's algorithmic engine continually compares SIGA's Level-0 sensor/actuator measurements with the values transferred between the PLC and the HMI, while factoring in synchronization issues like delays in communication, differing sampling rates, etc. Siga generates an alert when it detects any deviation between the two values for the same I/O at the same time.


SIGA
OT Solutions
SigaGuard
Reference
SMS
Email
SIEM
App
PARALLEL REFERENCE MONITORING
OT Network
Level 1
Data Packets
0101010101
Acquisition of Data Packets from Network
PLC
Level 0
Electrical Signals
Acquisition of Electric Signals
Digitization & Processing
Machine Learning Comparison Mechanism
Detecting deviations between Level 0 and Level 1 for each IO
Mission-critical Assets

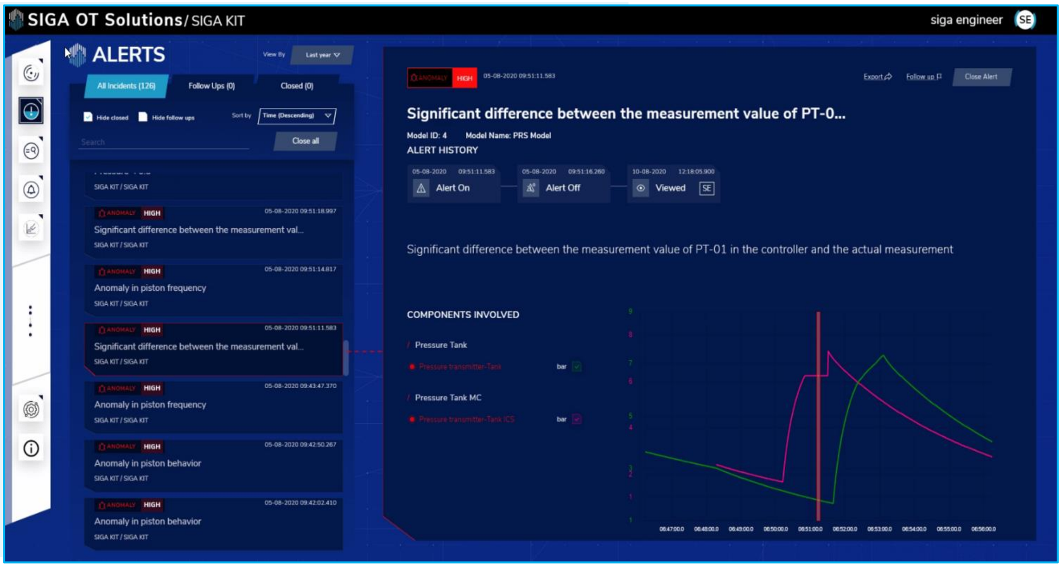
SIGA'S PRM ARCHITECHTURE

SigaSight DASHBOARD

Easy to install and use, SIGA's PRM provides immediate detection and alerts for cyber attacks on the PLC, even when the attacker is modifying parameters in an effort to blind the HMI. After the PRM is installed, a new screen will be added to SigaSight (Please see SigaSight™ User Manual for further details), showing in real-time the level 0 IOs values VS the ICS network IOs values:


SIGA OT Solutions / SIGA KIT
siga engineer
SE
PARALLEL REFERENCE MONITORING
113 ALERTS
TAGS:
☑ Limit switch piston - close position
☑ Limit switch piston - open position
☑ Compressor motor state
☑ Compressor relief valve (3/2)
☑ Piston relief valve (3/2)
☑ Piston operating valve (5/2)
☑ Green light lamp
1.000000
4.504
0.120
12:23:35.0
12:24:05.0
12:24:35.0
12:25:05.0
12:25:35.0
12:26:05.0
Time
TAGS:
☑ Limit switch piston - close position ICS
☑ Limit switch piston - open position ICS
☑ Compressor motor state ICS
☑ Compressor relief valve (3/2) ICS
☑ Piston relief valve (3/2) ICS
☑ Piston operating valve (5/2) ICS
☑ Green light lamp ICS
1.000000
4.503
0.158
12:23:35.0
12:24:05.0
12:24:35.0
12:25:05.0
12:25:35.0
12:26:05.0
Time

Once there is a deviation between the values, an alert will be triggered and displayed on the SIGA alerts screens.



SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:51:18.997
Significant difference between the measurement val...
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:51:14.817
Anomaly in piston frequency
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:51:11.583
Significant difference between the measurement val...
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:43:47.370
Anomaly in piston frequency
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:42:50.267
Anomaly in piston behavior
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:42:02.410
Anomaly in piston behavior
SIGA KIT / SIGA KIT

ANOMALY HIGH 05-08-2020 09:51:11.583

Significant difference between the measurement value of PT-0...

Model ID: 4 Model Name: PRS Model

ALERT HISTORY

05-08-2020 09:51:11.583 Alert On — 05-08-2020 09:51:16.260 Alert Off — 10-08-2020 12:18:05.900 Viewed SE

Significant difference between the measurement value of PT-01 in the controller and the actual measurement

COMPONENTS INVOLVED

Pressure Tank
Pressure transmitter-Tank bar ☑

Pressure Tank MC
Pressure transmitter-Tank ICS bar ☑