

PRM

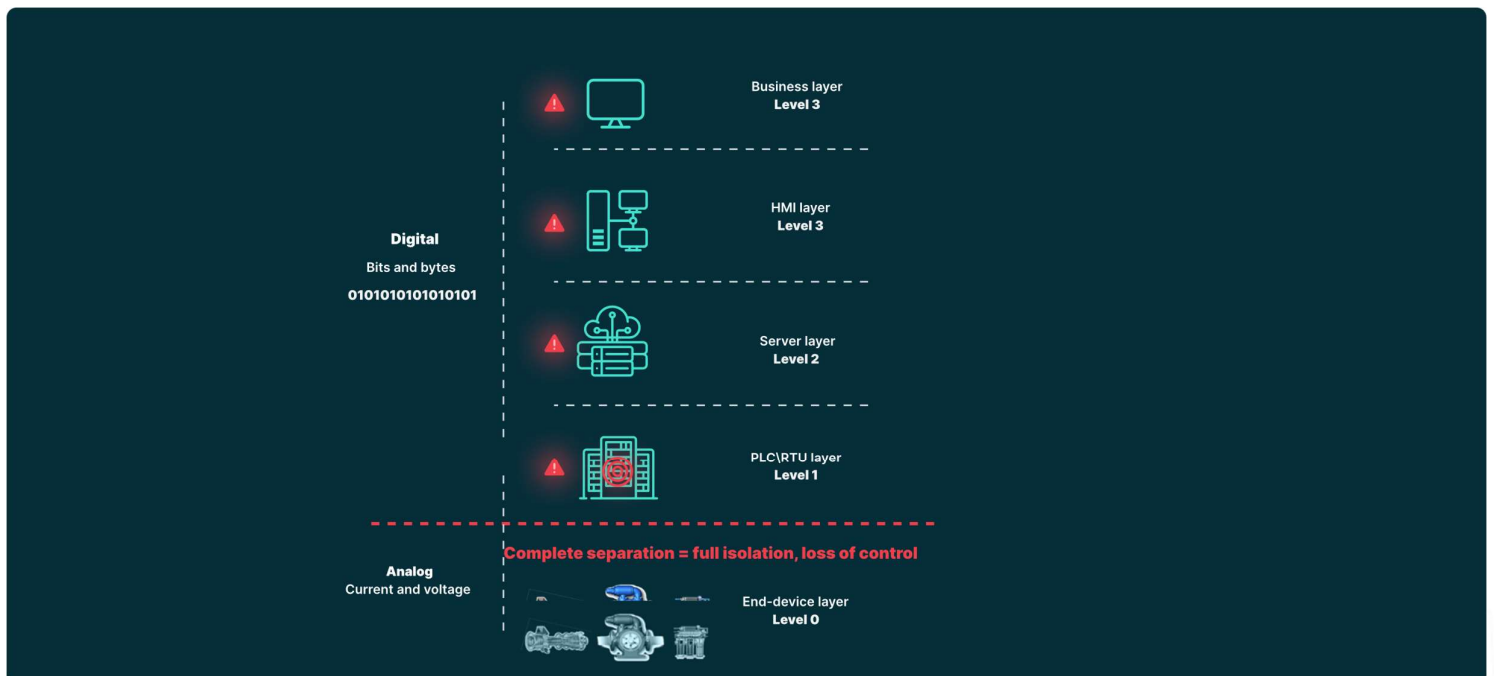
Parallel Reference Monitoring

BACKGROUND

Existing SCADA environments are increasingly being connected to the internet (IoT) and as a result suffer from particularly high limitations in the ability to apply even the most basic security techniques, common in IT environments. Current security techniques for industrial control systems are beginning to evolve and include network-level security, some use of firewalls, unidirectional diodes, and protected gateways. Nonetheless, these security techniques are designed to try and prevent unauthorized access via the Internet, yet leave the physical level, where the most critical processes are taking place unmonitored and thus unprotected.

This vulnerability and common operational constraint lead to very limited solutions, at best. Therefore, the SCADA's controllers' level, or Level 1 as it is called in the Purdue Model (e.g. PLC, RTU, etc.) can be compromised in various scenarios.

One of these scenarios (as illustrated in the figure below) is an attacker taking 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. This attack is known as HMI Spoofing and it is gaining popularity among hackers as their ability to "trick" the operators increases their ability to execute a successful attack for them and a disastrous one for the organization.







The control system's level 1, and the upper levels as well, will be basically "blind" to a process that happens in Level 0 (the physical layer) and the attacker can damage assets without any knowledge of the process's operators and without alarming the upper layers.

PRODUCT DESCRIPTION

The PRM (Parallel Reference Monitoring) solution is a new add-on product for SigaGuard, SIGA's flagship solution. It was developed in order to compare in real-time between what's really happening at Level 0 and what the operators are seeing in the HMI.

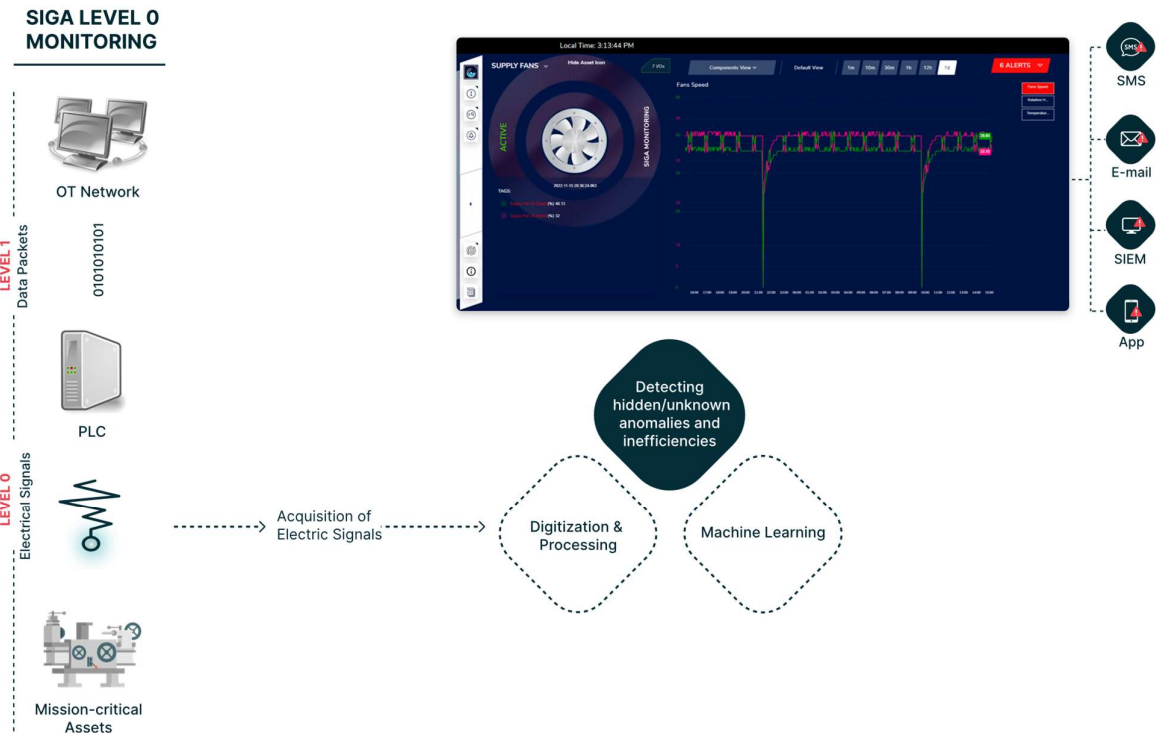
SIGA's algorithmic engine is constantly comparing SIGA's level 0 sensors/actuators measurements to the values transferred between the PLC and the HMI, while taking into consideration synchronization issues, like delays in communication, different sampling rates etc. The PRM add-on will alert when finding deviations between the two values for the same IO for the same point in time, possibly indicating some kind of cyber-attack or an operational functions in underway.

The prerequisites for the PRM are as follows:

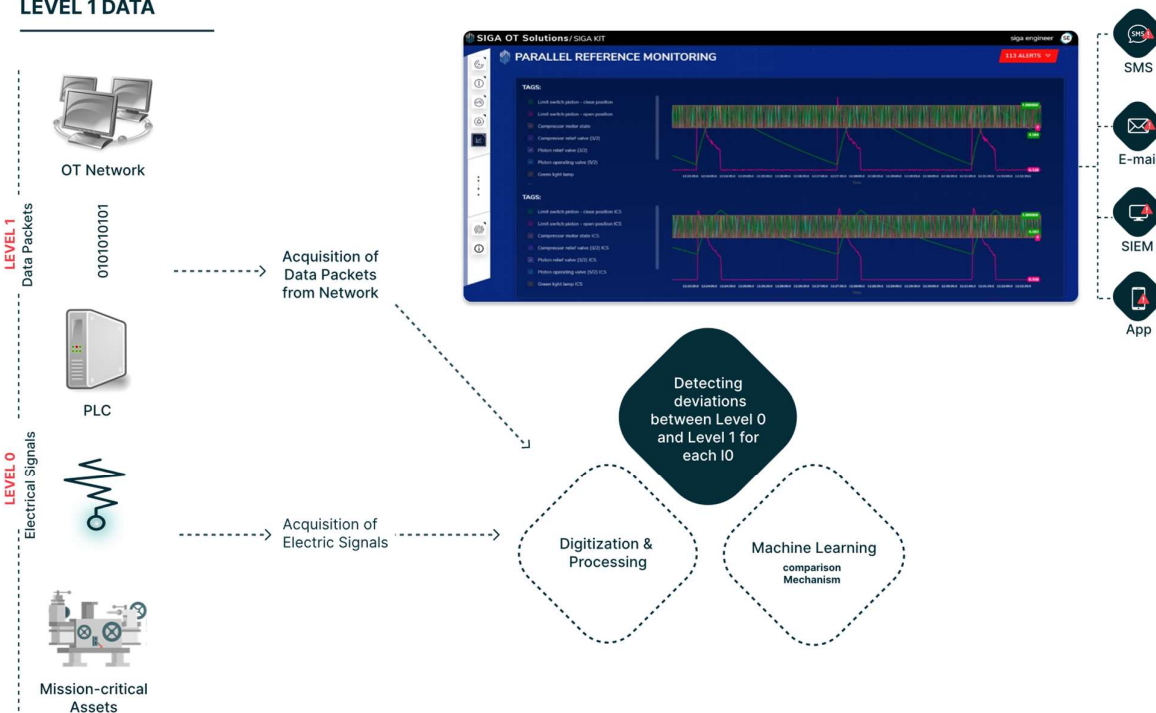
-  It requires SigaGuard to be connected to the customer's ICS/SCADA network switch in order to monitor the data going between the PLC and the HMI.
-  The IP addresses for the connected PLCs must be identical to the IOs SigaGuard is monitoring.
-  A list of the relevant registers of the IOs that SigaGuard is monitoring will be provided to SIGA by the customer.
-  A PRM software module and algorithmic model will be installed by SIGA on SigaGuard.



Below is the architecture of SigaGuard before and after installing the PRM:

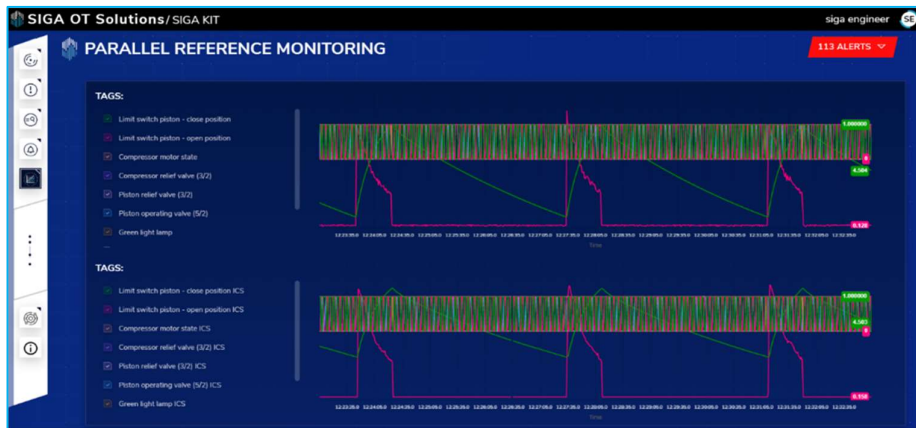


SIGA'S PRM ADDING LEVEL 1 DATA

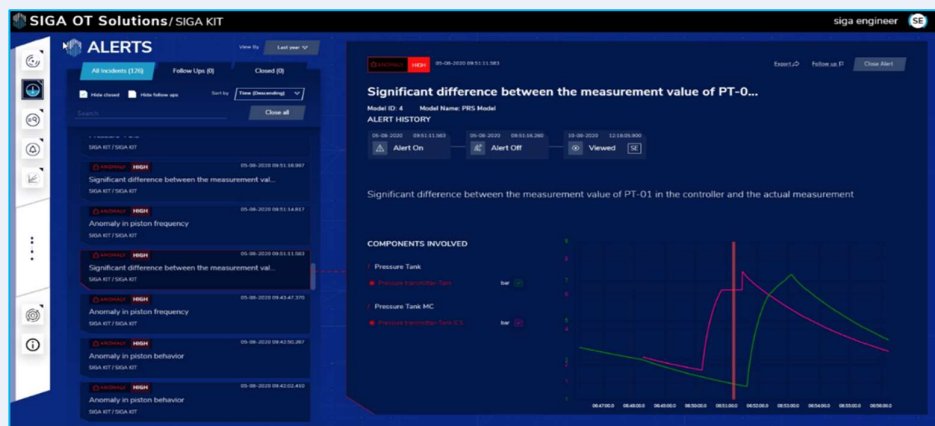


SIGA'S PORTFOLIO

After the PRM is installed, a new screen will be added to SIGA's dashboard (Please to the User Manual for further details), showing in real-time the level 0 IOs values VS the ICS network IOs values:



Once there is a deviation between the values, an alert will be triggered. The alert will be found in the regular alerts screen (Please refer to the User Manual for further details) and will be presented as follows:



SUMMARY

The PRM (SigaGuard Reference) provides the customer with great value of immediate detection and alerts on an almost certain cyber-attack on the PLC, caused by an attacker that is changing the process parameters and commands and "blinding" the HMI by presenting a false normal status to the operators. The PRM is simple to install and easy to use, the ideal add-on to ensure you can out-smart attackers and protect your critical operations and assets.