Overview

SCADAfuse is an inline network security appliance for the protection of industrial assets such as PLCs and network-connected machines and other devices. It first learns what workstations or other systems are permitted to speak to the protected assets, then identifies typical protocol usage between those nodes, and finally allows the operator to choose how deviations from those learned patterns are handled. A typical customer will filter or block errant messages which are not already identified as known and acceptable, and will configure the SCADAfuse to deliver its alerts to an HMI console for immediate operator visibility.

The following use case illustrates situations in which SCADAfuses brought immediate benefits to the industrial networks in which they were installed.

SCADAfuse Use Case: Drinking Water Safety

Customer Situation:

The customer is a midsized drinking water utility for a mid-sized city. They operate approximately 60 sites across their infrastructure, including four large pumping stations and a number of unmanned local service points. Consistent with local regulations, the drinking water supply is treated to maintain known levels of chlorine and a suitable pH level fit for human consumption.


The customer has rudimentary security (usernames and passwords) for consoles in their operations room, but once someone has access to the OT network itself, there are no additional protections. Thus anyone with network access could see and reconfigure any PLC or other asset anywhere in the treatment plant.

Customer Challenges:

- The customer wanted to ensure that PLCs could not be reconfigured by sources other than trusted workstations within the operations control center.

- The customer wanted to have a separate security control to validate that parameter values sent to injection pumps fell within known ranges, to protect against large spikes of chemical insertion into the water supply

Solution:

Remote HMI (Read Only)
HMI (Read/ Write)
Engineering (Read/ Write/ Configure)
SCADAfuse
PLC
Pump
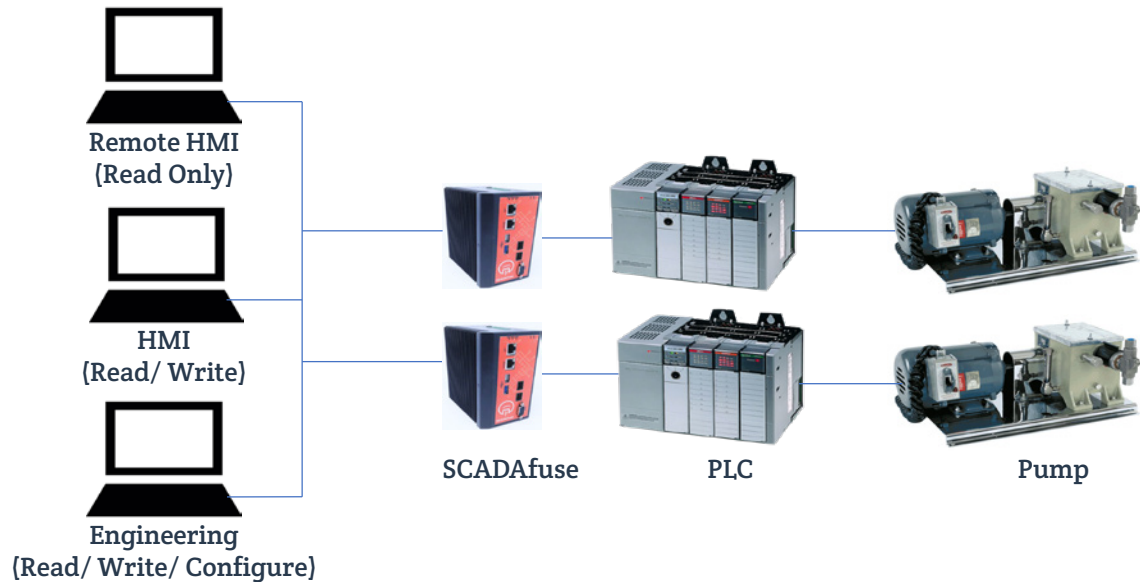
The customer selected SCADAfuse to be protect all critical PLCs, and certain network-connected industrial machines and other assets, and to report all their primary alerts back to HMI consoles within the operations control center.

During the initial learning phase, IP addresses and protocol usage patterns for interactions between trusted workstations and PLCs were confirmed.

In addition, SCADAfuse captured the typical parameters sent to injection pumps to regulate the rate of material injection.

Finally, the customer implemented operational procedures to ensure that the USB hardware keys required for SCADAfuse setup and reconfiguration were tracked using a physical log and stored in a cabinet which is monitored via a surveillance camera. The camera feed is recorded and also displayed in real time on a monitor in the control center, ensuring that a camera failure is immediately detected.

Upon final acceptance, the SCADAfuses were successfully protecting both modbus and ethernet/IP traffic such that only trusted sources were interacting via permitted methods with known critical PLCs and other assets. Any anomalous instructions to the injection pumps were flagged for immediate review and blocked from modifying pump behavior.

BAYSHORE

✉ info@bayshorenetworks.com

📍 Bayshore Networks, Inc.
4625 Creekstone Dr, #100
Durham, NC 27703

SCADAfuse
Industrial Controller Protection