SCADAfuse
Industrial Controller Protection

REMOTE MAINTENANCE OF MANUFACTURING SKIDS

## 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: Remote Maintenance of Manufacturing Skids*

## Customer Situation:

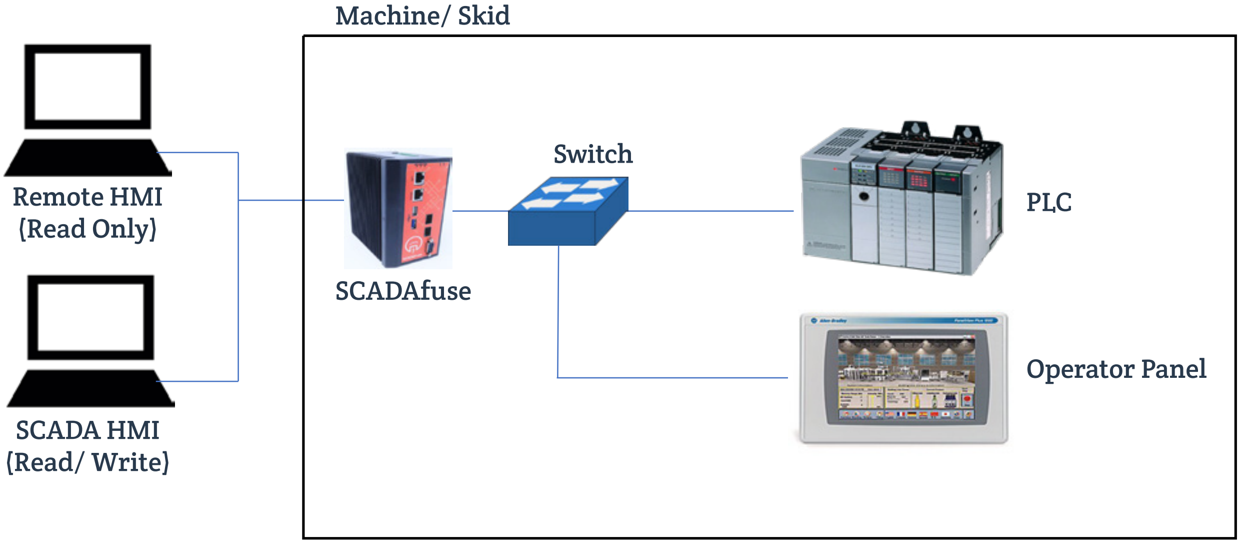
The customer operates a manufacturing system which is centrally managed via a SCADA network. The system includes machines ("skids") from a number of different manufacturers, each of which is able to perform diagnostics and maintenance on their own equipment at different times. The customer has no significant security controls between nodes within this manufacturing environment.

All network connections are hauled back to a single switching plane and are addressed on a single shared subnet.

## Customer Challenges:

- The customer wanted to implement virtual segmentation per-OEM/skid so that maintenance operations for one node could not inadvertently touch or impact nodes from other OEMs.
- The customer wanted to provide scheduled access control for overarching governance of maintenance activities to ensure they were only occurring during scheduled maintenance windows.

## Solution:



The customer selected SCADAfuses to define known source/destination permissions for access to individual skids by known individuals. The customer also defined maintenance windows for each supplier and maintained control over those schedule settings within SCADAfuse to enforce compliance.

During the initial learning phase, IP addresses for assets and workstations were identified and protocols used between management applications and assets were recorded. All other sources attempting to perform “write” type instructions were therefore excluded, and alerts generated if any violations were attempted.

Maintenance schedules were planned and agreed between suppliers and in recognition of the customer’s overall downtime scheduling practices. Certain shorter-duration windows were offered for limited activity types, while longer-duration windows were planned for more comprehensive updates and testing.

Upon final acceptance, the SCADAfuses were successfully enforcing virtualized network segmentation for the purposes of preventing OEMs from having any asset or network-level visibility beyond those assets which they were authorized to access. In addition, the scheduling enforcement features guaranteed that even with trusted access, maintenance could not be performed other than during the customer’s chosen maintenance windows.

BAYSHORE

info@bayshorenetworks.com

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

SCADAfuse
Industrial Controller Protection