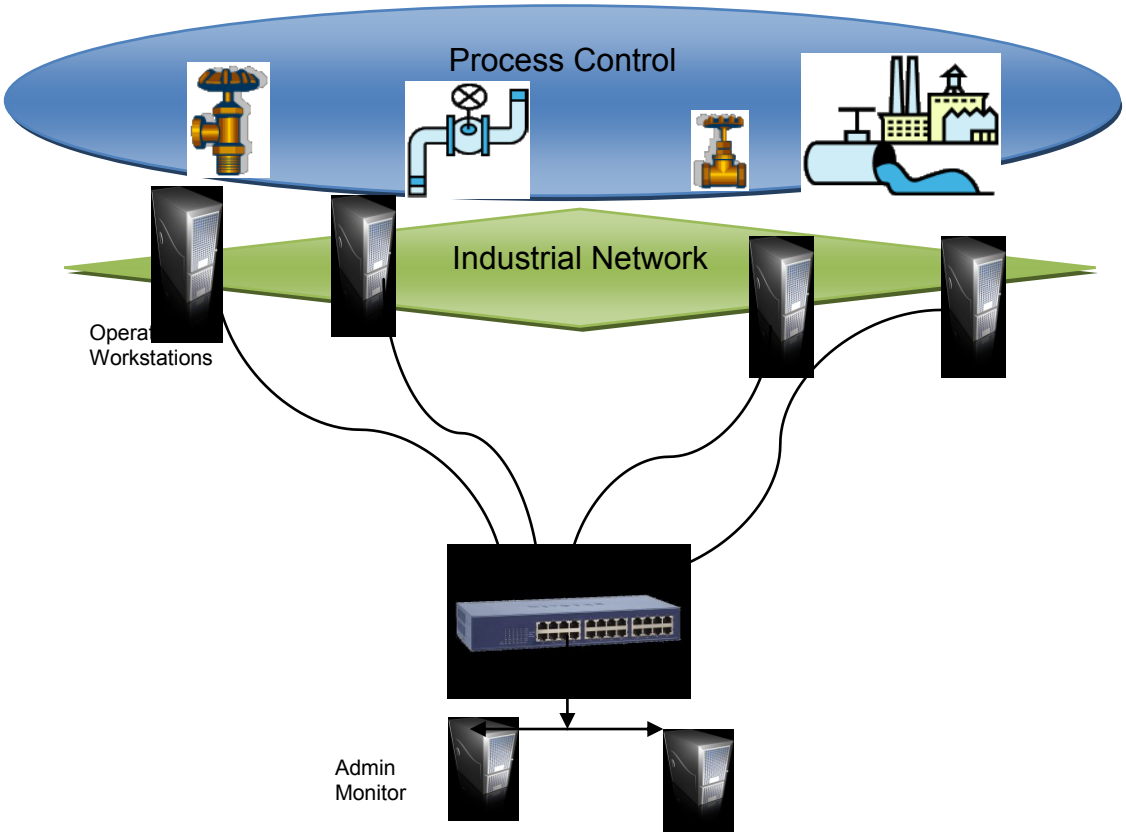
AROW Data Diode

Using AROW with Rsyslog

Domain boundary protection can be a problem for sysadmins who need to collate information from multiple sources, for example operational to enterprise networks.

The utility rsyslog is often used to enable the system logs from multiple sources to be sent to a single admin monitor. The utility can tag and filter user logs, so that they are easily recognisable at the monitoring point



But of course this system without protection is prone to security breaches including hi-jacking of the controller network.
A data diode can provide a guaranteed air-gap for these processes and AROW supports rsyslog transmissions with very little or even no extra effort.

Rsyslog can be very easily configured to work with UDP or TCP carriers.

UDP

In the case of a single UDP, this can be routed directly through AROW with no further equipment or processing required. Simply create a conf rule, for example
‘ *.*@x.x.x.x:514’,
save it as e.g. 10-rsyslog.conf in /etc/rsyslog.d and all future local syslog entries will be routed to the chosen ip address.

Multiple UDP sources require a switch with a single connection to AROW.

Using AROW with Rsyslog

Rsyslog settings:

On the rsyslog monitor, edit the /etc/rsyslog.conf file and add (uncomment) these lines:

$ModLoad imudp
$UDPServerRun 514

In order to create a new log for each client, add a template using the lines:

$template RemoteLogs, "/var/logs/%HOSTNAME%/%PROGRAMNAME%.log"
. ?RemoteLogs
&~

The rsyslog docs explain these settings.

You will also need to change file permissions on the destination log path so that syslog can create new logs, e.g.
(sudo) chown syslog:syslog log
or whatever works in your system.

Now simply add the AROW ip addresses to your routing tables and you are done.

TCP

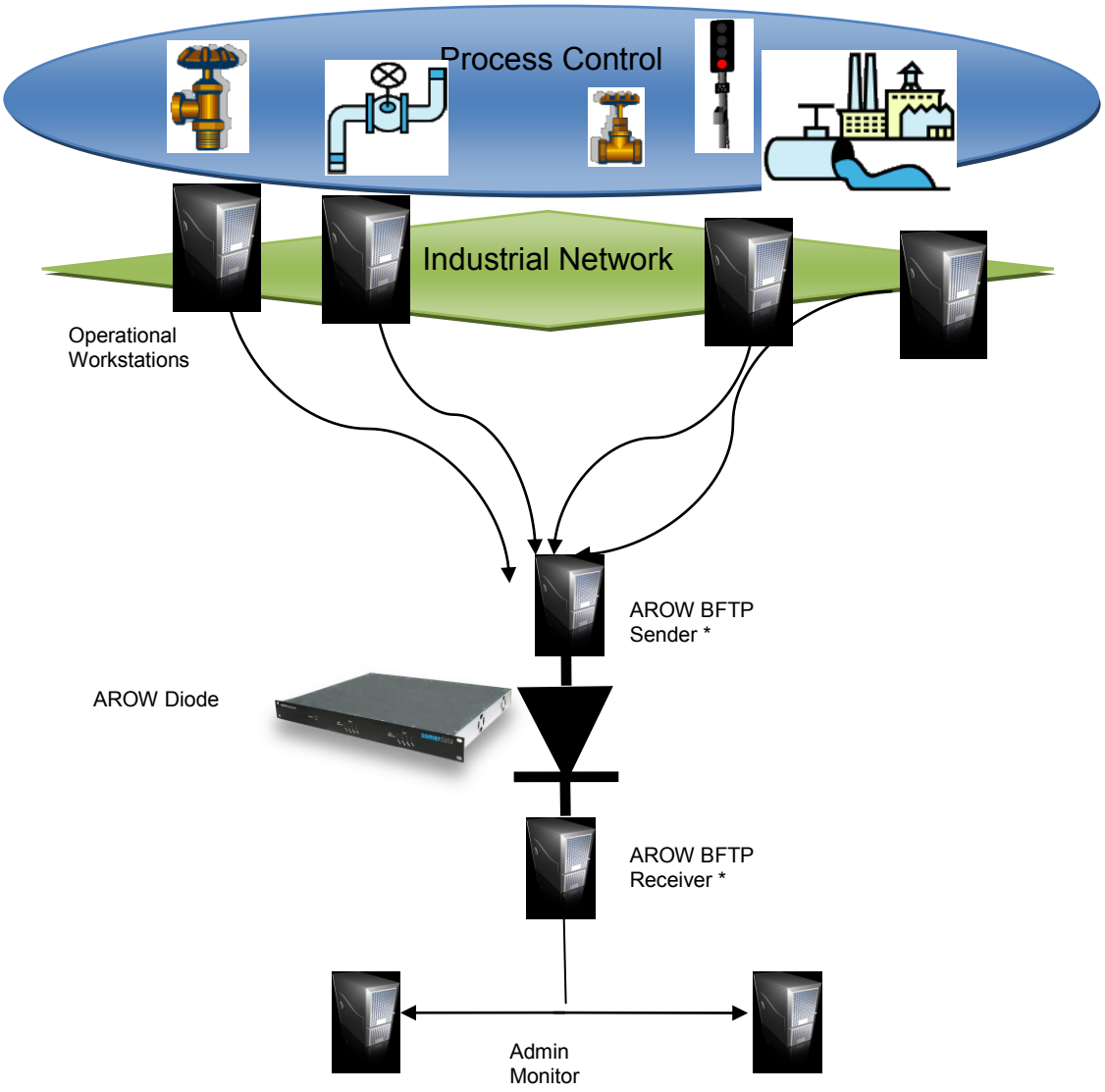
For multiple TCP clients, change the file created above to tell rsyslog to use the TCP protocol e.g. *.*@@x.x.x.x:10514 and on the monitor machine add/uncomment the
$ModLoad imtcp
$TCPServerRun 10514
lines

Now you'll need to use the free python scripts on each side of the diode to handle the TCP streaming data from multiple clients. See the manual for details.

AROWBFTP handles all of the network connections, making the route transparent to connected devices, while AROW provides absolute air-gap security between the networks.

Your network diagram now looks like this and has completely secured your operations from outside attack.

Using AROW with Rsyslog



* These Python scripts can be hosted on any convenient platform (eg one of the clients and monitor systems) – dedicated devices are not always required

somerdata

Somerdata Ltd
1 Riverside Business Park
St Annes Road
Bristol
BS4 4ED
UK

Phone: +44 (0)1179 634050
E-mail: sales@somerdata.com
Website: www.somerdata.com