CHAMPION TECHNOLOGY SERVICES

CASE STUDY:

How Industrial Network Segmentation Can Resolve Critical Issues

How one facility improved network security, saved money and remained compliant by employing Network Segmentation

Collaborate › Innovate › *Accelerate*

www.ChampTechnology.com

AN INTRODUCTION

Most networks are a flurry of traffic. Too much data transfer can cause issues, both with functionality and security. Network segmentation can help mitigate risks to your control system.

When a refinery experienced mystery communication loss, causing missed alerts and emission data, Champion implemented network segmentation to secure the network and bring it into compliance.

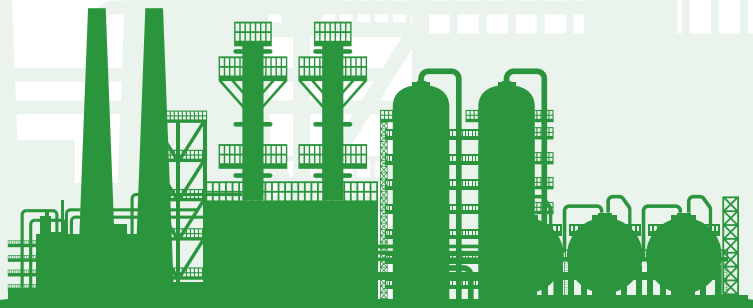
THE CUSTOMER

A top-level oil and gas refinery was using a DCS & PLC system to control multiple flares. Data related to emissions and noxious levels of gasses provided by the flare analyzers were displayed on a PC workstation. Control staff were required to monitor these levels and report any "out of norm" values to management and proper authorities, including the DEQ and EPA.

THE PROBLEM

Communication Dropout with Flare and DCS
The customer's operations personnel reported intermittent communication losses to the devices on the network, particularly with the flare analyzers. With no communication from the flare analyzer, site control system personnel had no emissions data to monitor. Communications loss occurred over multiple hours during each drop out instance.

The customer identified these network loss issues as a major problem. No data means they could not detect nor report if any emission issues had occurred. After initial troubleshooting, the staff could not isolate the problem. At that point, the customer's Process Automation Control Manager called in Champion Technology Services to investigate and resolve the network issues.



CHAMPION ANALYSIS

Champion performed a site survey and visually inspected all network equipment inter-connections, analyzed network architecture drawings provided by the customer, and evaluated the implementation against industry/manufacturer best practices.

Our personnel also thoroughly investigated the issue by connecting to every switch and PLC on the flare analyzer network to evaluate the device

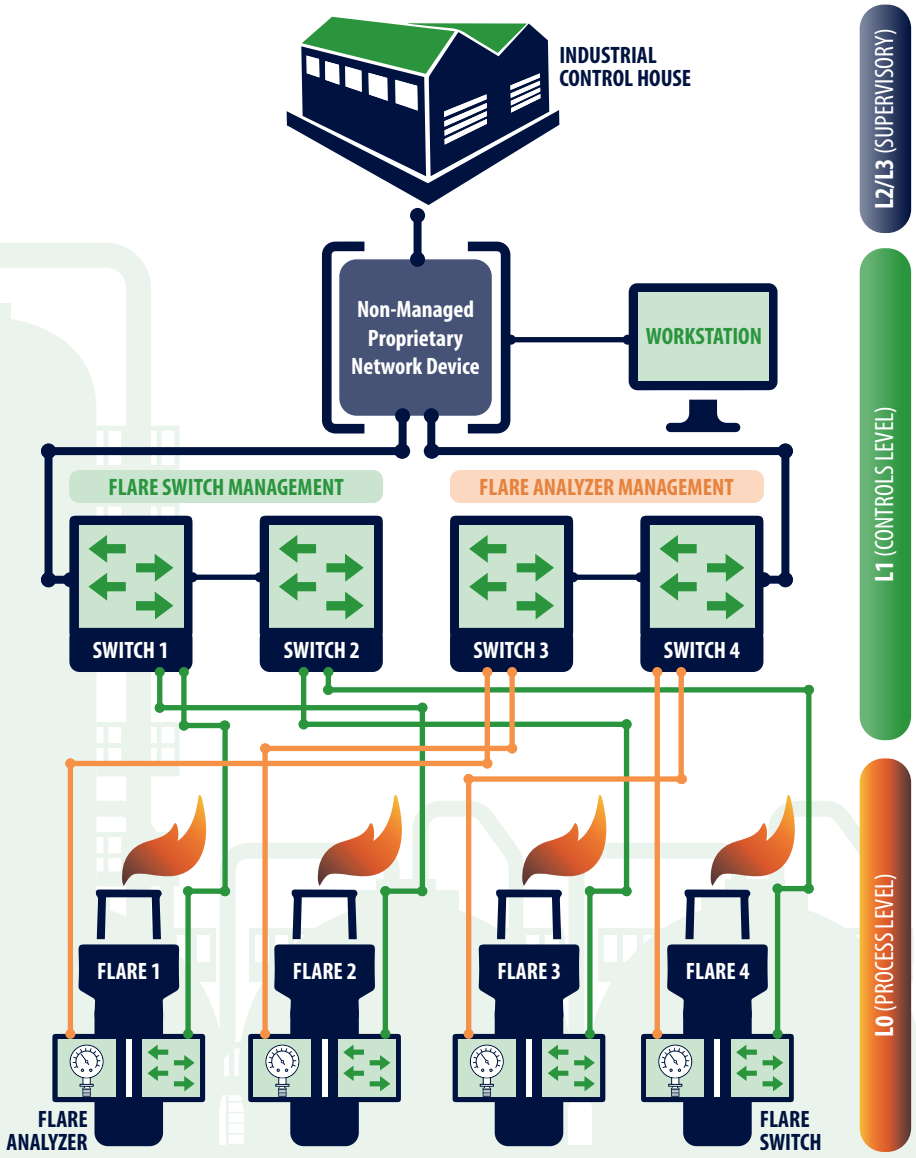
What We Found:

All communication from the flares to the DCS ran through a non-managed, proprietary network device. This configuration is outside of generally accepted best practices and posed a potential threat to the security of the control system.

There were no redundant connections between the switches, resulting in a single point of failure if a fiber link were to fail.

Switches used on the network did not support multiple required protocols used to establish optimal communication between the flare switches in more complex networks. The flare network devices were ignoring or improperly handling the data.

FLARE AREA NETWORK (BEFORE)



CHAMPION SOLUTION

Network Segmentation and Issue Tracking

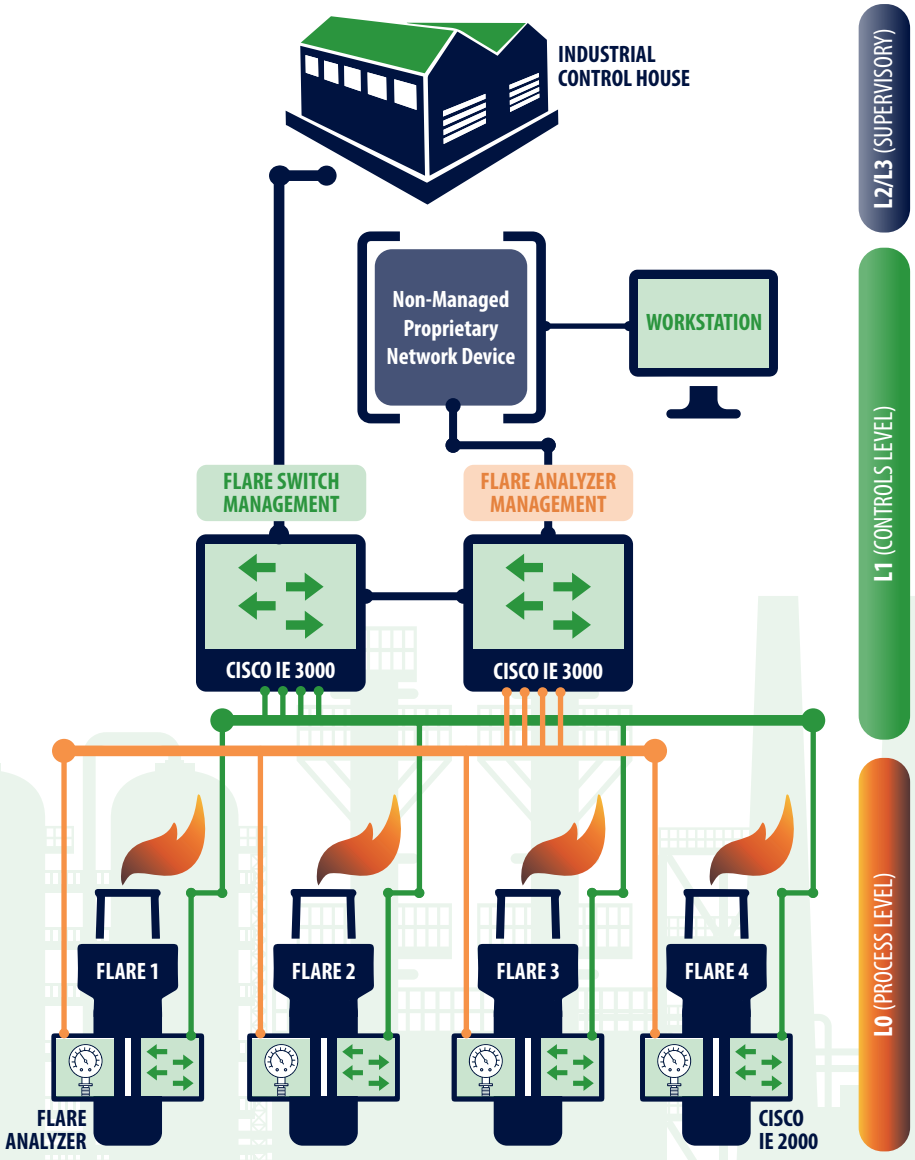
Network segmentation involves isolating or splitting off subnetworks to boost performance and improve security.

Through segmenting the network and the application using industry-standard equipment, Champion restored confidence in the reliability and performance of the flare analyzer network. With the addition of a Syslog system, the customer now has data for monitoring and troubleshooting.

Solution Highlights:

- Replaced low-function switches with Layer 2 managed switches that support all required protocols required to handle data between the flares and the DCS.
- Segmented the flare network away from the non-managed, proprietary network device as per industry recommend configuration standards. The unmanaged switch as the gateway to the higher-level network could have led to unpredictable performance and was a security vulnerability.
- Reduced network traffic and increased available bandwidth by enabling protocols on the new switches. This also optimized the pathing between all switches on the flare network and higher-level networks.
- Installed Syslog software on a network workstation to monitor traffic. This provided a means to capture data for future troubleshooting and incident investigation.
- Trained customer site control personnel on the new system. Specifically, they were trained how to conduct initial troubleshooting and perform switch maintenance.

FLARE AREA NETWORK (AFTER)



Going Beyond the Initial Solution

Champion found the root of the communication problem and resolved it by implementing cybersecurity and Operational Technology best practices. In addition, we worked to prepare our customer for unknowns that may occur in the future by providing on-site training. By installing the Syslog software, customer personnel now have the tools they need to monitor and troubleshoot network issues.

A reliable and more secure control system means control staff will be alerted if an emission issue occurs, and the customer won't pay hefty environmental fines for violations they never knew happened.

Want to learn more?

Champion's **ISA and GICSP Certified Cybersecurity Experts** are trained in the latest ISA/IEC 62443 standards for Cybersecurity.

For more information, or to schedule a consulation, contact:

Sales@ChampTechnology.com

CHAMPION TECHNOLOGY SERVICES

11824 Market Place Avenue
Baton Rouge, LA 70816
Ph: 225-291-5548
Sales@ChampTechnology.com

OFFICES

Baton Rouge, LA
Beaumont, TX
Denver, CO
Houston, TX
Lafayette, LA
Lake Charles, LA
New Orleans, LA
Salt Lake City, UT