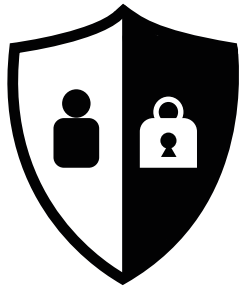


Alderley



Technical excellence: delivered



Case Study

Project Type: Cyber Security Upgrade

Introduction

Our client, a globally renowned gas company, operates some of the world's largest LNG production and export facilities.

The challenge

To upgrade and protect a total of 4 LNG trains, consisting of 18 control rooms and 24 custody metering skids.

There are many efficiencies from an increasingly digitalised and connected world. However, there are also many threats due to system vulnerabilities and malicious cyber-attacks.

As with any process system, unplanned downtime of an operator's flow computer and control system can have a significant impact on operational and bottom-line performance.

Accordingly, our client requested a full review and upgrade of their metering control and operating systems, with a particular emphasis on cyber security.

This to support the continued operation of this globally important LNG facility and to reduce the risk of downtime caused by potentially malicious cyber activities.



The solution

An independent domain control cyber security network - the first to be installed by a metering system integrator in the Middle East.

Having worked closely with the client to support a full metering control system upgrade, Alderley had extensive knowledge of their systems and operating infrastructure. As a result, there was no requirement for an initial inspection and system audit on this occasion.

Utilising this intimate system knowledge, our cyber security and control system experts developed and built a functional, secure and resilient closed network to operate and protect their assets - in full compliance with Industrial Control System (ICS) regulations.

This solution includes:

- Control measures across areas such as user access permissions and device lockdown policies. This gives all individuals the correct access they need to perform their daily tasks, whilst ensuring that non-approved devices or users are unable to access or modify any systems.
- Physical and logical resilience built throughout the infrastructure to ensure zero impact to production in the event of a system hardware failure.
- Continuous monitoring using System Logging tools to dynamically reports events. Where response times are critical, they are applied at all levels across the infrastructure.
- Periodic backups across all servers. This includes the backup of data in a full-differential format to enable the full restore of a server or any minor restore requirements at file level.

The result

Two key factors underpinned the entire development:

- ensuring that it complies with Operation Technology Cyber Security standards ISA 99 / 62443.
- that it is functional from an output perspective; ensuring the upgraded systems are fit for purpose and continue to support effective and efficient operations.

Since implementation, the client has reported zero cyber security incidents and their metering control system continues to operate effectively and efficiently.

Alderley has since been asked to provide further control system and cyber security upgrades at our client's other facilities, including upgrades on equipment originally supplied by another provider. This is testament to the quality of service provided by our cyber security and control system experts.

