Asset Guardian®
SOLUTIONS LIMITED

# CASE STUDY

## Cyber Security Management System Software Solution for one of the World's Leading Oil and Gas Operators

# BACKGROUND

A major Oil & Gas operator undertook to protect itself from the increasing threat of cyber attack. In order to do this, they sought to comply with the industry standard **IEC 62443**.

It comprises standards, reports and procedures pertaining to Industrial Automation and Control Systems **(IACS)** cyber security, in a controls and automation environment. The area that was required to meet the standard consisted of nine offshore sites and two onshore.

The main challenges faced by the Oil & Gas operator were:

- As their systems became more integrated, they became increasingly vulnerable to cyber security threats e.g phishing, water-holing, randsomware and malware.
- These threats could be launched from anywhere and from apparently trusted sources.
- Offshore facilities were becoming more vulnerable due to forms of potentially unsecured connections such as USB, Wi-Fi and Bluetooth.

# SOLUTION

The **IEC 62443** standard is written to combat these threats and it specifies the use of a **CSMS** (Cyber Security Management System), a robust cyber security framework. A **CSMS** defines the business's entire cyber security strategy, which includes the use of computer based systems to track everything related to protecting against all forms of cyber attack.

The oil and gas operator was already aware that they had Asset Guardian installed on all of their onshore and offshore sites. It was being used to provide a single repository for storing the data of programmable systems, supporting access to data both on and off shore which provided effective PLC code management as part of its disaster recovery strategy.

After review, it was decided Asset Guardian would be used as the system required as part of the CSMS as defined in **IEC 62443.**

## THE RESULT

Not only was the network architecture in place, a wealth of data and information was entered into the database that already filled many of their requirements.

Asset Guardian’s approach to handling access, logging and managing information and system software was well suited for use as a CSMS.

Asset Guardian offered the functionality to manage cyber issues such as patch levels and software upgrades, identifying cyber risks and improving business continuity.

In the event of data loss, software could be restored from the leader server. The leader in turn was backed up at a secondary onshore site as part of the disaster recovery plan.

The use of Asset Guardian as a CSMS as part of the overall cyber security strategy ensured the operator was adhering to IEC 62443.

**Used by Leading Oil and Gas Operator**

**In compliance with IEC 62443**

**Installed across 11 sites**

**Disaster Recovery**