The information age and birth of the Industrial Internet of Things (IIoT) has delivered a wealth of opportunity in terms of process efficiency for critical infrastructure industries, but it has left the systems which control these processes open to malicious attack. Designing and implementing a resilient industrial control network requires core competencies in both cyber security and industrial automation. Recently there has been a cross-industry development in the way companies view cyber security; stakeholders are awakening to the threat posed and following the change to IEC 61511 the ultimate liability and direct accountability for the security of critical systems stops at board level.

Increasing dependence on technology, the convergence of IT (Information Technology) and OT (Operational Technology) infrastructure has opened the door for intruders and the oil and gas industry is particularly vulnerable.
Servelec Controls is bridging the knowledge gap between IT and OT environments by working with clients on a consultative basis to ensure that IT compliance and the impact on control systems and process networks is fully understood.

Servelec Controls is currently working with BP on their Andrew field located 230 kilometres North East of Aberdeen to update the production and drilling platform’s legacy control system. The field started production in 1996 and had an initial expected field life of 19 years. The legacy system, which in some parts was decades old was not designed to protect against the modern cyber security threats that exists today. The Control, Monitoring and Safety System (CMSS) on BP Andrew is a bespoke system with no known contemporaries and several key system components are no longer manufactured and have been given a finite support life from suppliers. The CMSS is currently supported, maintained and modified by Servelec Controls.

As part of this work, Servelec Controls is modifying the legacy Siemens PLCs to interact with a new HMI being installed by Emerson. As part of the design and development of the system, the Servelec Controls designed system will ensure secure communications between the HMI layer and the PLCs controlling operations on the platform.

Ensuring secure communication between the HMI layer and operational PLCs is done by deep packet inspection on the network communications between each PLC and the HMI layer of the control system, performed by a ruggedized firewall. The firewall blocks any unauthorised communication for either control instructions being fed to the PLC or information being fed back to the HMI layer and generates alarms to inform the operator.

By utilising functionality provided within the firewall device, the system is protected from unauthorised communications which can manifest itself in several forms. Communication from unknown devices on the HMI network are blocked by the firewall which protects against rogue devices communicating with the PLCs. In addition deep packet inspection prevents the HMI from issuing commands or requesting data from registers which are not in the approved list configured in the firewall. This configuration provides assurance that the Modbus PLC communications are robust and resilient from unintended external interference.
The consequences of a cyber security breach for an oil and gas producer are severe. Consequences such as plant sabotage, interruption to supply, production disruption, terrorism and undetected spills are more than just an inconvenience; each could quite possibly result in loss of life, severe environmental pollution and irreparable damage to plant. To protect against current and future cyber security threats Servelec Controls always adopts best working practice for the design, development and implementation of every solution delivered, as standard.

As an independent integrator, Servelec Controls has a wide-ranging automation platform knowledge and is competent and certified to install and support most of the world’s leading OEM’s portfolio of products including ABB, Emerson, GE, Invensys/Schneider, Rockwell and Siemens. With Servelec Controls, you have a partner who understands the operational technology landscape, the vulnerabilities attackers seek to exploit and what needs to be done to protect national infrastructure from inevitable threats.

To find out more about Servelec Controls’ cyber security solution visit servelec-group.com/servelec-controls/solutions/cyber-security/ or email enquiries@serveleccontrols.com.