

Cybersecurity Solutions

For offshore topside Cameron BOP control systems

APPLICATIONS

Offshore rigs using topside Cameron BOP control systems

BENEFITS

- Enhances operational integrity of topside Cameron BOP control systems
- Shields BOP control system from cybersecurity threats
- Compatible with existing Windows® XP and Windows 7 software configurations
- Seamlessly integrates to maximize uptime
- Uses same graphical user interface as your previous system
- Implements best practices from National Institute of Standards and Technology (NIST) and International Electrotechnical Commission (IEC)

FEATURES

- Operating system using Windows 10 Long-Term Servicing Channel (LTSC)
- Application whitelisting
- Wonderware® SCADA platform
- Administrator features and component password protection
- Security configuration management for USB
- Services available to manage operating system security and patch updates
- Verification and validation using independent third-party industry experts performing modeling and intrusion testing
- Human machine interface (HMI) that conforms to existing control panels

Shifting from isolated security measures to a more connected cybersecurity solution, Cameron now offers a cybersecurity-enabled system that focuses on both operational integrity and data security of offshore assets. Based on the Connect IQ* drilling equipment life cycle management services concept and the firewall network that accompanies it, the cybersecurity-enabled system protects Cameron topside BOP control systems against possible and unintended cybersecurity threats. Verified and validated on our newly commissioned state-of-the-art BOP controls simulator, the cybersecurity-enabled system maximizes uptime of your offshore drilling rig.



Cybersecurity-enabled Cameron BOP control system simulator.

The robust, configurable cybersecurity-enabled system seamlessly retrofits BOP control systems with a Windows 10 operating system and firewall-protected network. The system can be installed and commissioned either at one of our many service locations or offshore during nondrilling periods.

The new cybersecurity-enabled system is fully backwards compatible, whether you want to update an entire system or replace a single HMI. A full cybersecurity suite upgrade includes new HMIs for your Drillers Control Panel (DCP), Tool Pushers Control Panel (TCP), Supervisor Control Panel (SCP), as well as new computers for Eventlogger, Connect IQ Historian, portable electronic test unit (PETU), and BOP test box.

Cybersecurity Solutions for Cameron BOP Control Systems

Features	Existing BOP Control System	Cybersecurity Enabled
Operating system	Windows XP, Windows 7	Windows 10 LTSC
Supported operating system	Obsolete Q1 2020	Viable to year 2025
Feature updates	Monthly	Every 2 to 3 years (with option to delay or skip update)
System hardening min.	None	Operating system security hardening with Center for Internet Security® Benchmarks™ Bloatware and unused services removed Least privilege security policy Security logging
Application whitelisting	None	Microsoft AppLocker®
USB protection	None	Security policies
User access control	None	Nonprivilege account for normal operation, administrator account reserved for update and maintenance
PLC and Ethernet switch	None	Password protected

*Mark of Schlumberger
Other company, product, and service names are the properties of their respective owners.
Copyright © 2019 Schlumberger. All rights reserved. 19-DRL-615790