DATA SHEET

OWL Cyber Defense

Securing Real-Time Monitoring for BSEE Compliance

What You Need to Know

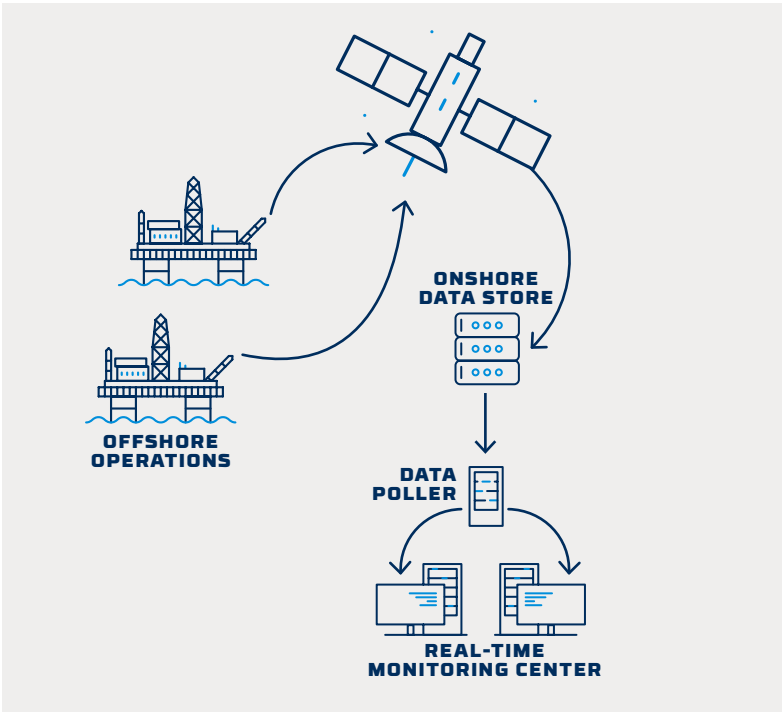
In April 2016, the **Bureau of Safety and Environmental Enforcement (BSEE)** published the final Well Control Rule[1] which includes key new requirements for Real-Time Monitoring (RTM) in offshore rig operations.

Operators are required to gather real-time data using an independent, automatic, and continuous monitoring system capable of recording, storing, and transmitting data regarding:

- The BOP control system
- The well's fluid handling system on the rig
- The well's downhole conditions (with the bottom hole assembly tools, if any are installed)

This data must be sent to an onshore facility during operations for proper monitoring and response capability and also must be available to BSEE upon request.

These requirements went into effect April 29, 2019.



Why is the Well Control Rule Being Implemented?

In response to the Deepwater Horizon disaster in 2010, the U.S. Department of the Interior launched a series of aggressive reforms. Among them, the BSEE RTM requirements in **30 CFR §250.724**[2] reflect the changing offshore oil and gas environment and are designed to uphold national interests in safety, security, and environmental protection. Because events that are critical to safety and environmental regulation during well drilling and completion are largely related to pressure management, these requirements are directed at collecting and sharing critical Well Control and Integrity Data when conducting "well operations with a subsea BOP or with a surface BOP on a floating facility, or when operating in a high pressure, high temperature (HPHT) environment." Where operationally reasonable, RTM may be deployed to help predict and prevent these kind of critical equipment failures and compare operational data across multiple sites in real time.

Cybersecurity Implications

Cyber threats against critical infrastructure, such as the energy industry, are growing exponentially and proper cybersecurity in offshore oilfield operations is a necessity. In potentially dangerous environments such as offshore well drilling, the growing connectivity and merging of OT and IT mean that safety and cybersecurity are now inherently interlinked. As the RTM requirements could potentially open an external network pathway for cyberattack, it is vital that operators evaluate cybersecurity from a risk-based perspective to ensure their networked infrastructure monitoring and control systems address cybersecurity, critical access points, and resilience.

[1] *https://www.govinfo.gov/content/pkg/FR-2016-04-29/pdf/2016-08921.pdf*
[2] *http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=500aaf93a47ec84baff9ab4b6cb2d250&ty=HTML&h=L&mc=true&r=SECTION&n=se30.2.250_1724*

What You Need to Do

Beyond the safety implications in the original intent of the RTM requirements, the ability to remotely monitor the vast amounts of data available to you (up to 2 TB of data every day) can have a dramatic impact on cost effectiveness, operational up-time, and overall productivity. As such, you will need to develop and implement a real-time monitoring plan (to be available to BSEE upon request). This plan must include documentation and consideration for the following:

1. **RTM capabilities, including data types to be collected from monitored activities.** This may encompass many different aspects of the rig and drilling tests. The following are the primary events and activities that should be monitored:
   - Wellbore Positioning
   - Blowout Preventer (BOP) Testing
   - Casing/Liner Pressure Testing
   - Formation Integrity Test (FIT)
   - Leak Off Test (LOT)
   - Positive and Negative Pressure Tests of Well Barriers
   - Cementing and Zonal Isolation
   - Drilling Margin Events
   - Station Keeping

2. **How RTM data will be transmitted onshore during operations.** Typically, offshore facilities would transmit via satellite back to onshore facilities, although these connections can vary. Considerations include transmission technologies and capabilities, meeting bandwidth requirements, and preventing data outages and redundancy.

3. **How RTM data will be stored, labeled, and monitored by qualified onshore personnel.** In most instances, this will involve some sort of data monitoring or response center with its own dedicated data repositories. As previously mentioned, the amount of data generated can be very high, so considerations for properly storing this data should include the possibility of offsite or cloud backup.

4. **How you will provide BSEE access to onshore monitoring facility and data** (if applicable, the location of any onshore data monitoring or data storage facilities) and your procedures for, and methods of, communication between rig personnel and onshore monitoring personnel.

5. **An action plan if you were to lose any real-time monitoring capabilities** or communications between rig and onshore personnel, and a protocol for responding to significant or prolonged interruption of monitoring or onshore/offshore communications (notifying BSEE to be included in protocol plan).

Securing RTM Data Transmission Against Cyberattack

Due to the safety implications of a potential cyberattack against rig systems, it's vital that operators outline and implement proper security for RTM data transfer. Firewall software-enforced security is popular across many industries for its familiarity and low up-front cost. However, the need for frequent updates and heavy ongoing management make them a problematic choice for offshore facilities where specialized personnel are at a premium and equipment may be shared across multiple vendors and managed by still more. Data diode hardware-enforced network security technologies provide a simple, reliable, and highly-secure means to transfer data one-way for onshore monitoring without the need for heavy ongoing management or frequent software updates. Their ability to function for extremely long periods (10+ years MTBF) and unhackable nature make them a very attractive choice for future-proofing RTM security for offshore facilities.

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com