xage SECURITY

SECURING OIL & GAS EXPLORATION, DRILLING, AND PRODUCTION

Use Case

Oil & Gas exploration and production is data intensive and often involves multiple parties. A typical drilling rig may involve multiple contractors and subcontractors, each responsible for separate parts of the operation and each with their own subsystems and data sets. It's an expensive and risky undertaking where effective and real time data exchange is of critical importance.

The various parties lack the means to share data safely, flexibly and securely. Cooperation is restricted both by the risks of cross contamination in the event of a cyberattack and by the need to establish trust in another party's data integrity. Sharing data securely between the various systems and parties is a major undertaking. Each responsible party on the rig implements and operates their own systems and networks in order to protect themselves from malware, malicious actors, and data theft. These separate systems make it difficult to exchange vital process data needed to improve the efficiency and safety of the rig operation as whole.

At best, data is separately assembled then passed to centrally located experts, like lab based geologists, versus exchanged directly between systems in the field. Enabling real-time, bi-directional data flow between parties and systems in the field along with the central offices can save millions of dollars, but also improve the health and safety of everyone involved. Incidents such as spills and explosions (e.g. Deep Water Horizon) can also be a side-effect of inadequate communication and information exchange.

Common Data Exchange Challenges:

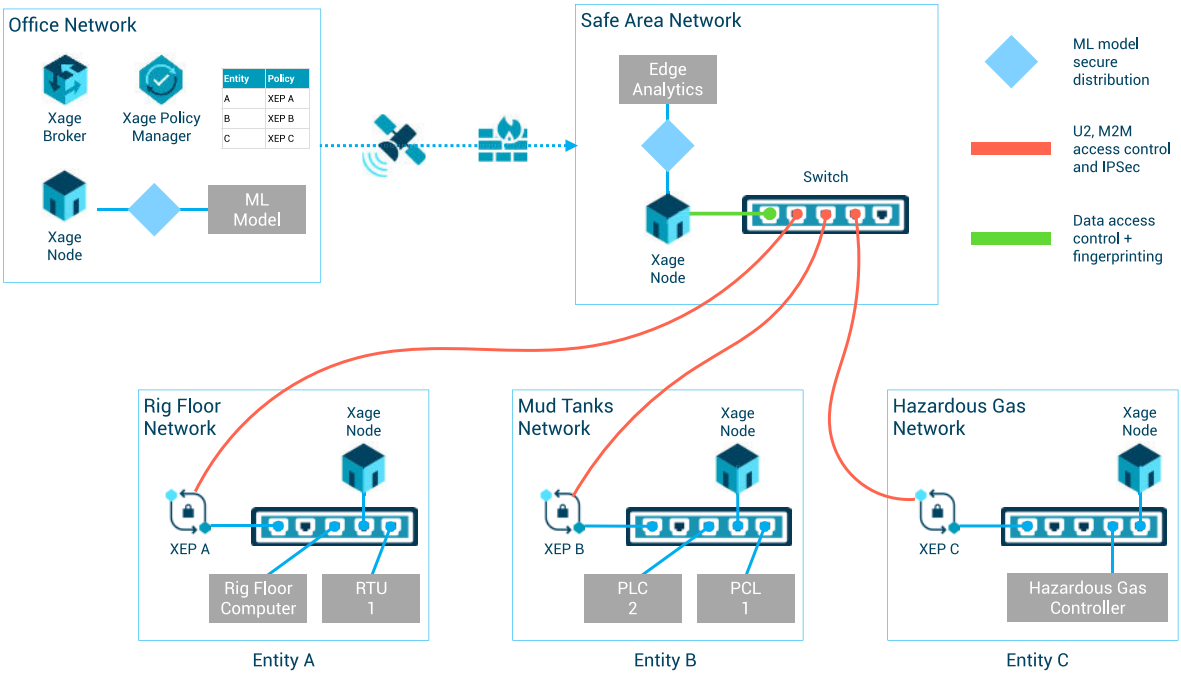
- Multiple isolated networks and systems (between contractors on rig side and backend oil company systems)
- Low bandwidth and high latency communications often utilizing satellites from rigs to backend systems making it difficult to analyze in the center
- Unsecured industrial protocols and systems with limited role-based access control to the data and encryption capabilities
- Network segmentation via security zones leaves the individual zones vulnerable to in-zone attack
- Multiple parties involved in the operation that may not fully trust each other, are reluctant to give up control of their own data, and may not want to rely on the integrity and accuracy of data supplied by other parties.

xage

Xage Security Fabric is a blockchain-protected identity & access management and data security solution that enables multi-party cooperation with granular control over data interactions and end-to-end data authenticity, integrity, and privacy.

- Secure data sharing and analysis at the edge across multiple parties and systems
- Granular control (down to each data value) for data sharing policies by each entity/party
- Role and protocol based control over all system interactions governed by each entity
- Common authentication platform for user and machine access to data and systems
- Data fingerprinting at the source to ensure authenticity and integrity across the operation
- Immutable and tamperproof record of data reads and writes
- End-to-end granular and automatic data encryption in-transit & at-rest even across multiple data stores
- Irrefutable access control policy and tamperproof record that can be validated by all parties

Xage builds trust across multiple entities and secures all machine, user, app, and data interactions rig, control, and enterprise.



About Xage Security

Xage Security is the universal security solution for industrial operations, creating the essential trusted foundation for every interaction, whether human-to-machine, machine-to-machine, or edge-to-cloud. Xage protects all equipment, delivering identity management, single sign-on, and access control with in-field enforcement across the operation. Xage is the first and only blockchain-protected security solution providing tamperproof, non-intrusive protection and enabling efficient operations and innovation across multiple industries.

Xage Security
445 Sherman Avenue, Suite 200
Palo Alto, CA 94306