Red Hat Enterprise Linux transforms the edge in oil and gas

Edge computing delivers the ability to deploy compute power to locations where it was never before practical. Combine edge computing with the cloud and you have a significant technology shift. Its potential has companies looking for innovative places where they can insert new digital capabilities into traditional approaches.

Energy companies face barriers to edge computing

While technology continues to transform industries, companies often fail to adequately prepare for the challenges of scaling their transformation. Lack of preparation causes promising solutions to fall short of business expectations.

In the energy vertical, barriers include unique requirements for:

- Device classification.
- Cybersecurity.
- Infrastructure security, which includes protecting the safety of workers and nearby communities.
- Operational reliability.

While all industries are looking for strategies that promote advanced business logic via technology, the oil and gas sector has requirements that few others share. Exploration and production operations take place in a variety of environments, including offshore platforms and remote locations far away from developed areas. Refineries seek strategies to minimize downtime and ensure worker safety. Environmental concerns demand the flawless operation of supervisory control and data acquisition (SCADA) systems. Retail outlets seek competitive advantage through digital initiatives—from contactless pump operation to smart delivery of information and services to customers' devices and cars.

The quest for technology-enabled performance improvement has been part of the oil and gas industry for decades. The greatest strides, however, are fairly recent, in the form of lower computing costs, smaller device footprints with larger storage and memory capacity, an explosion of open source edge messaging and data science packages, and improvements in public and private network connectivity. Edge computing is the latest, and possibly most significant, technology influence.

Edge computing allows on-the-spot computing and analytics throughout the oil and gas value chain. Combined with private and public cloud capabilities, this capability can result in a significant shift in the industry. Enterprise executives and managers in field, refinery, and retail operations are considering how to take advantage of the technology.

Compute and storage escape the firewall

Energy organizations are using edge computing solutions to build remote monitoring capabilities for their assets. This approach will allow performance improvement across a range of operations, including predicting equipment issues to optimize maintenance operations, validating and enforcing safety protocols, and assuring physical plant security. Currently, edge solutions are geared toward autonomous production, artificial intelligence (AI)-assisted drilling, and optimized field operations. These solutions are being delivered through a new class of devices with Intel Atom or Advanced RISC Machines (ARM)-based chipsets with multiple interfaces that can connect to low-cost sensors. They

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

facilitate digital transformation by gathering data and communicating with other networked computers and cloud platforms. They can also control other "things" at the network edge, either autonomously or with direction from engineers in remote locations.

Edge computing goes beyond simply augmenting operational technology (OT) through the Industrial Internet of Things (IIoT) with devices downwell or on pipelines. When energy companies combine cloud computing with the power of distributed computing devices, they gain localized computing power to execute complex and often data-intensive applications and processes in any location.

While edge computing can fundamentally change how oil and gas companies improve performance across the value chain, it also introduces challenges for IT departments and technology vendors. For decades, companies have processed the majority of their data within the physical security of a datacenter and behind a corporate firewall. As technology has evolved, data gathering, analysis, and storage have extended beyond the datacenter and firewall. With edge computing, these actions can happen in the datacenter, in the cloud, or at the data source. Decentralized computing architectures present a number of challenges, including cybersecurity concerns, sourcing needed skills, and determining how to sync OT and IT.

As they approached this new distributed frontier, the supermajor IT team faced a major hurdle. They needed to envision how to load an operating system designed to run in the datacenter onto a device that lives in the field, with security and at scale.

Oil supermajor takes a transformational journey to the edge

Recently, a supermajor announced plans for aggressive growth, pushing to double its earnings without changing customer pricing. Given this ambitious goal, the corporation launched another level of digital transformation initiatives. As the supermajor began developing a new architectural design, it became clear that conventional ways of thinking no longer applied. Building a platform that could meet the requirements of a decentralized world while building upon existing internal knowledge would require new ways of doing things.

The supermajor needed to determine how an operating system (OS) could provide IT capabilities while also solving intricate field-level issues encountered during exploration and production. The IT team needed to devise a way to load an OS designed to run in the datacenter onto a device that lives in the field. Among other considerations, the team looked at how to perform patching, maintain the security of the OS itself, and ensure recoverability. These and other challenges would require new approaches because IT staff could not just walk to the server as they would in a datacenter.

Red Hat provides critical expertise in embedded and edge computing

It also became clear that central processing unit (CPU) architecture support was an important capability in the longer term. Having both Intel and ARM support for a given OS provided the ability to design once and then devise an implementation plan that could accommodate power, size, and price, depending on the use case. As the team rounded out its needs and refined the architecture, they turned to Red Hat to help navigate the world of embedded and edge computing.

Red Hat had invested in the edge computing and IIoT space for years through work in multiple open source community projects. The Red Hat® team pointed them to a Fedora® project that was unique in that it addressed how IoT would require a different approach to the OS. The supermajor and Red Hat worked together to define the necessary components needed to achieve this vision. Furthermore, they offered a blueprint for these improved capabilities to the entire Linux® community.

The original design targeted consumer use cases, such as computer vision, data collection, and general processing. Surprisingly, the architectural design and thought that the team put into the various components also helped to guide their counterparts in the operational technologies domain. Much of their work directly supported—with minimal rework—the transition from IT to OT use cases.

This transition provided commonality of both skills and a technology solution. It also helped the organization's business partners focus on their requirements. It allowed them to have an architectural design that included a Red Hat Enterprise Linux operating system.

Red Hat Enterprise Linux at the edge

Edge computing requires thinking differently about security, resiliency, operational patterns, and how operating systems provide value. The decentralized nature of edge computing raises the stakes and amplifies a number of risks. For example, routine tasks like reprovisioning and accessing a remote console are simple in cloud and datacenter environments. Accomplishing the equivalent scenario for remote edge environments can require customers to send a nontechnical resource to the site. Security comprises another challenge as hardware exists away from the datacenter. Edge devices tend to be physically more accessible and vulnerable to threat vectors compared to assets in a traditional datacenter.

An array of technologies and management techniques make Red Hat Enterprise Linux perfectly suited to handle the workload demands, security needs, and environmental challenges of edge computing in the oil and gas industry.

Linux containers provide an operational separation of concern

In recent years, Linux containers, specifically Open Container Initiative (OCI)-compliant containers, have become the preferred approach for deploying and managing applications. The technology has become a critical building block to most modern architectures. While the benefits of using containers were initially focused on cloud computing, the same value proposition is equally applicable to edge and IIoT environments.

Container images distribute applications with all their runtime dependencies as an immutable atomic unit. This structure has the effect of making applications extremely portable. It also means that the life cycle of applications can be managed independently from the underlying operating system. This decoupling not only provides much greater flexibility of application dependencies but also creates a smaller, more focused contract between the kernel -> container engine -> container process.

This contract vastly minimizes the possibility of traditional maintenance and patching processes to negatively impact containerized applications. It relieves IT administrators as, when appropriate, application teams can also control the deployment and rollout of their workloads while infrastructure teams can ensure that the underlying OS is maintaining security updates with far less risk to the applications.

Containers also provide a number of security benefits. The Linux kernel offers extensive sandboxing capabilities for processes that, in practice, are rarely used on their own. Containers make it simple to use features like cgroups, namespaces, SECCOMP, SELinux, and to restrict the underlying surface area of the system that is accessible to applications. The implementation of container security makes a secure-by-default posture easily obtainable.

Adapting Red Hat Enterprise Linux for the edge

Historically, IT teams have used two primary approaches for distributing Linux in edge and IIoT environments. The first involves an embedded approach that treats the OS more like firmware. Advantages to this model can include a small footprint containing only the binaries necessary for the environment, an A/B partition update model, and consistency across devices. While this offers a valid approach, it also has commonly encountered drawbacks, including a lack of visibility into the included binaries. Embedded distributions can appear as a mystery, and unfortunately some of these fail to deliver security updates for the life of the system.

Challenges around introspection, common vulnerabilities and exposures (CVE) analysis, and complying with corporate standards also create barriers for operational systems to connect to IT-owned infrastructures. This model is also criticized for being inflexible and difficult to adapt over time. Altering the OS or firmware may require the end user to create their own custom build and take ownership of the operating system compile, testing, and deployment. This option is not realistic for many use cases and introduces more risk than reward.

The second approach involves using a traditional package-based distribution. Similar to the prior example, it has numerous advantages, including adaptable installs that can change with your environment's needs, simple introspection, and IT compliance. Conversely, a standard distribution can also be challenging to manage and keep consistent at the level of scale seen in edge and IoT environments. Over time, drift between systems creates scenarios that can increase the cost of management and lead to fragile environments.

While each approach has its merits, a technology called rpm-ostree introduced through the Fedora IoT project, can provide the best of both of these approaches. The rpm-ostree is a hybrid image and package system that combines the features of libostree and libdnf. This technology allows for transactional updates of images and packages where only the deltas are used to compose a custom Red Hat Enterprise Linux OS. Through close customer collaboration, Red Hat Enterprise Linux-supported packages can be used to construct a fit-for-purpose Linux edge operating system designed with the imagebuilder tool built from rpm-ostree supported repositories. This approach combines the reliability and consistency of an A/B-style update model, with the security and life cycle of Red Hat Enterprise Linux content that enterprises trust. These rpm-ostree images are simple to customize and adapt as needed by the environments in which they operate. Why redeploy the entire OS or ship a new device when you can make changes centrally and easily push them to production in minutes?

Network efficient OS updates with intelligent rollbacks

Network efficient OS updates, also known as transactional updates, dramatically improve the resilience for OS updates and ensure that nodes are always in a "known-good" state. Greenboot uses rpm-ostree and application-specific tests that can be run on startup. In the event of an issue, the system will rollback changes and preserve the working state. This feature helps eliminate the need to choose between application stability and applying security updates. In addition, it eliminates the need to physically touch the edge device in case of a failed patch or update.

The update payloads for rpm-ostree are highly optimized for intermittent and low-bandwidth connections, transferring only a fraction of the data used by a traditional package-based distribution.

Linux containers and rpm-ostree have matured over recent years. Red Hat and many other companies across different communities have worked to unite efforts and solve common challenges in this space.

Creating a more efficient and more secure edge computing architecture

The supermajor and Red Hat created an efficient and more secure architecture for edge computing in oil and gas. This architecture helped the company make headway toward its aggressive business goals, and it also helped to reduce business risks. In addition, it offered combined IT and OT benefits, such as enabling teams to patch devices at scale and mitigating business risks like bricking a remote device during an update.

Red Hat Enterprise Linux offered the ideal foundation for this new platform, making it easier for the supermajor to manage containers—and gain the inherent security benefits.

Learn how Red Hat helps organizations transform their edge computing infrastructure.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F27858_0521