Jumpstart Connected Strategies

Remote monitoring reduces costs, improves uptime, and jumpstarts connected strategies. Integrated platforms enable a flexible path, protecting both edge and on-premise computing options.

By Ed Trevis, Corvalent

Application-ready platforms act as building blocks to the Internet of Things (IoT), providing a secure development path that speeds time-to-market and assures flexibility as needs sway between centralized and de-centralized computing. Tapping into these platforms to enable remote monitoring and management capabilities is an ideal first step toward an IoT-based future.

> "To streamline the overwhelming nature of creating an IoT system strategy, OEMs and developers should address a primary use case such as remote monitoring and management as a first step."

The IoT can present a number of roadblocks for OEMs and application developers. The impact of committing to network technologies, development platforms, cloud providers, and more, means that a misstep could become a costly setback. Such a misstep might not even reveal itself until an application needs to scale or a security breach demonstrates a performance limitation. These are the kinds of factors that keep technology innovators awake at night, even while they are fully aware of missed opportunities resulting from a lack of real-time connectivity between systems and applications.

To streamline the overwhelming nature of creating an IoT system strategy, OEMs and developers should address a primary use case such as remote monitoring and management as a first step. By capitalizing on integrated hardware/software platforms optimized for flexible development, the path to connectivity is both straightforward and secure.

Tapping into Remote Monitoring

Accessing remote monitoring and management capabilities is a good place to start, with the potential to deliver fast value from an IoT investment. While deployed systems represent a wealth of potential data, many are not yet equipped with sensors and applications that enable data to be gathered and shared in a timely fashion. Even if performance data is currently being gathered, it may not be actionable quickly enough to support predictive or preventive maintenance.

Figure 1: Based on Intel® x86 processors, Corvalent's CorEdge box PC product family offers a powerful, flexible, and reliable platform, helping developers reduce time-to-market, protect application security, and support reliable performance. Each application-ready system can be customized to the individual needs of the project, including software pre-installation, hardware installation and configuration, and system branding. Systems can be shipped "ready to plug-in" to manufacturing facilities, or directly to end users in non-branded packaging. (Image credit Corvalent)

The win comes from accessing and sharing that data in real-time. If a system is running hot due to environmental issues or looming component failure, proactive measures can be taken only if operators are made aware of the rising issue. In another example, a system may be performing well and even exceeding its anticipated quota of scans or cycles; consider a high-performance MRI machine quickly reaching a milestone for number of scans completed. Ideally it should warn operators in advance that maintenance is soon required, before unexpected downtime costs hospitals thousands in unrealized revenue.

An application-ready integrated platform enables OEMs to configure these remote monitoring applications quickly, adding sensors to aid in predictive maintenance operations for the end-user. Integrated platforms may also ship with sensors on board, enabling remote monitoring out of the box.

Solving Risk Factors

Achieving system longevity is an important part of the design goal—saving millions of dollars over the life cycle of a product based on reduced costs in hardware and software compatibility testing, qualifying and validating new platforms, and agency re-certification. With IoT technology investments, embedded OEMs and developers face additional risk, as the pendulum constantly swings between centralized and de-centralized computing. Solving this significant challenge involves working with an application-ready platform that is inherently flexible. Developers can embrace any type of IoT environment, tuning system performance to the edge or on-premise without a change in architecture. Ideally, software can be deployed in any manner that makes sense for the application at hand.

This advantage allows developers to reduce risk dramatically, removing difficulty by building their applications on what could be called 'infrastructure middleware.' Across the full spectrum of embedded applications—industrial automation, medical, defense, energy, and more—most technology leaders compete best by focusing on their business of managing large devices or systems, not building core level platform middleware.

Addressing Pain Points and Simplifying Deployment

It is true that engineers love to build things, but their bosses need to build the bottom line. Given that time-to-market is a critical factor in this effort, application-ready platforms address a range of options that improve the balance between costs and development resources.

End-users want to put software where they need it, and avoid being tethered to one cloud provider vs another. Rather than committing an infrastructure build to a cloud service such as Amazon, Google, or Azure, an integrated 'container-based' IoT platform can be deployed and moved as needed. Edge components act as self-contained IoT systems, and can run completely disconnected from the cloud or the on-premise server.

Improved Reliability with Security at Every Layer

This flexibility and independent capability also protects uptime, for example in scenarios where a rugged system may not have connectivity. The device continues to operate under the rules running at the software edge, an important value add for non-stop applications such as manufacturing or hazardous security.

Security innovations capitalize on options built into processors such as hardware-accelerated encryption; today, a range of features is available below the operating system, creating comprehensive capabilities that enhance productivity and secure management. In an integrated system, secure hardware dovetails with secure software. The perspective is 'security first,' with protocols architected into the platform at every opportunity. Everything is locked down by default, and developers must specifically open ways to access the system. This is in contrast to ground-up solutions, where security tends to be an afterthought—it is typically handled in the opposite fashion, with developers having to make choices about which protocols to turn on.

Security faults arise when the development takes place, and security decisions follow. It is much more effective to incorporate a secure mindset as part of the development effort itself. This allows the system to be secure and interoperable at every layer.

Developers in Mind

An optimized platform is built with developers in mind, using open architecture and a full range of communication interfaces. Most interface protocols are available, as well as open source protocols and APIs for communicating with devices or enterprise systems. Developers are empowered to focus on the business problem at hand, building their solution as opposed to building a low-level infrastructure.

Your IoT Initiative

Tackling a single mission such as accessing remote monitoring and management capabilities is a smart strategy, right-sizing the overwhelming proposition of becoming IoT-enabled. These capabilities not only reduce maintenance costs, but also make OEMs more competitive for their end-user customers. Because deployed systems can be supported remotely, costly on-site visits to either repair or simply diagnose systems are vastly reduced. Uptime is improved with more proactive options, and overall support resources are significantly better managed based on predictive and preventive maintenance strategies.

Integrated hardware/software platforms provide the necessary tools—as well as the freedom—to enable this value for developers. Faster time-to-market, reliable performance, and a security-first perspective are bundled in a flexible system that accommodates both edge and on-premise computing. Investments are protected with longevity in mind, capitalizing on the remote management platform as a flexible IoT framework on which to build additional connected applications.

This initial step can open the door wide for what's next. The ability to create IoT systems in a fast, scalable, secure manner may be just what it takes to move your organization into the future.

Ed Trevis is President and CEO, Corvalent. Trevis has been Corvalent President and Chief Executive Officer since the company's inception in 1993, leading the firm to double-digit growth, rapid gain in market share, and numerous business awards and recognitions. He is an active CEO member of Vistage International, and maintains a leadership philosophy promoting employee education and encouraging personal and professional growth. Connect with Ed via LinkedIn or at ed.trevis@corvalent.com