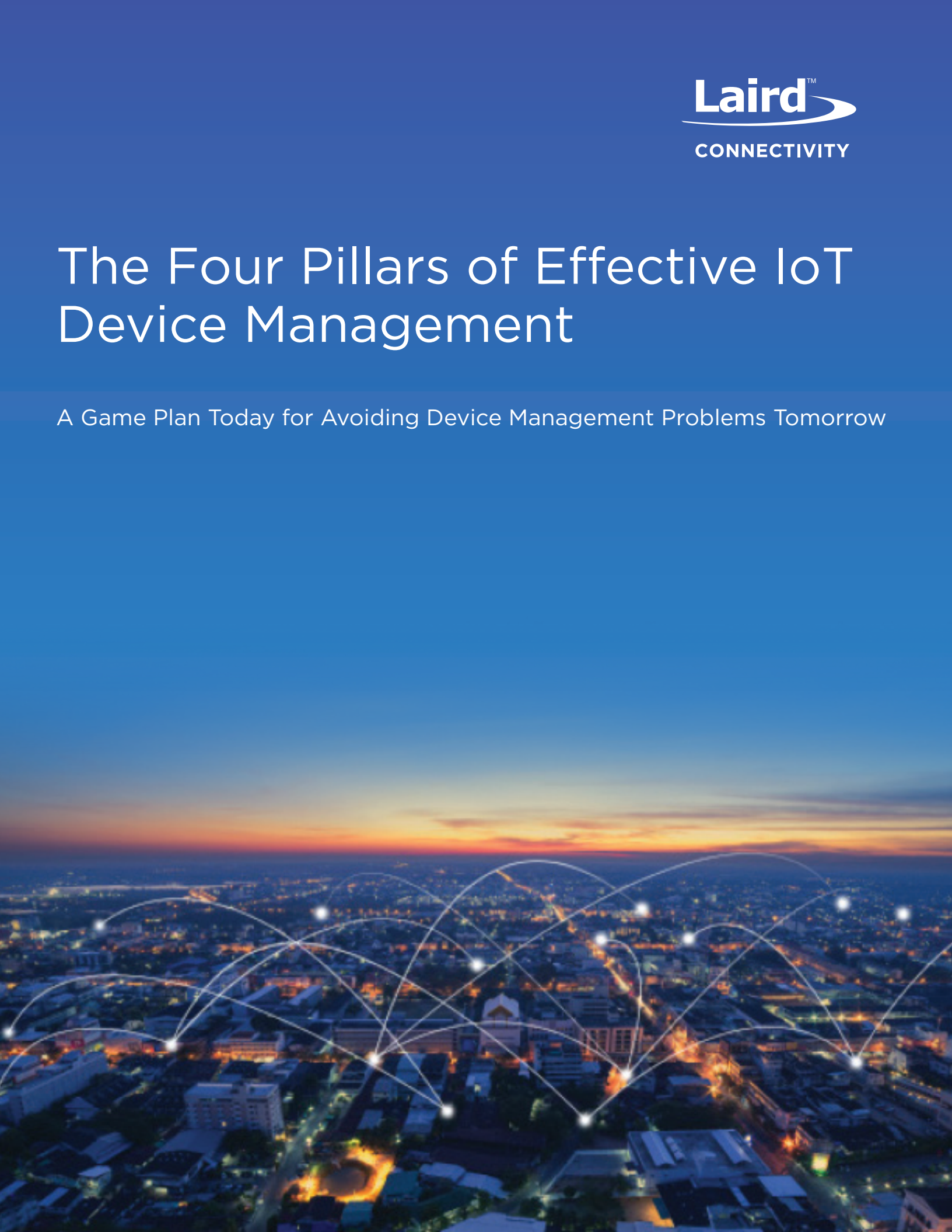
Laird™
CONNECTIVITY

The Four Pillars of Effective IoT Device Management

A Game Plan Today for Avoiding Device Management Problems Tomorrow

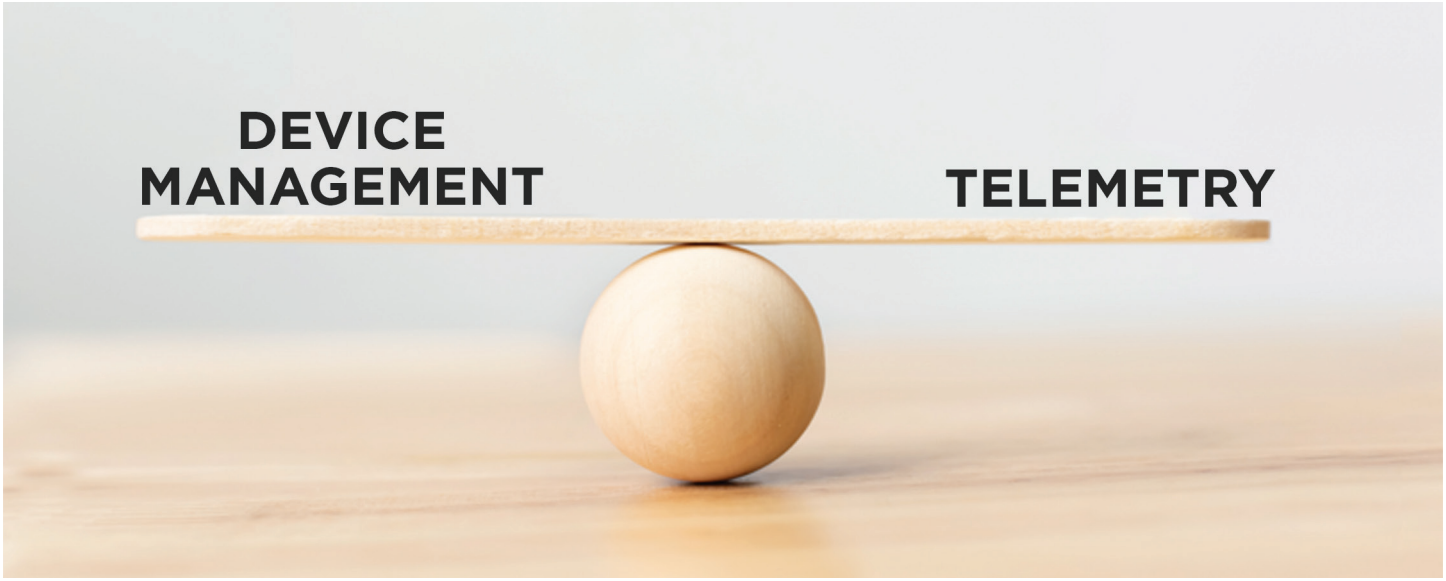


The results are in, and it's no contest. No issue in the world of IoT is as confusing and misunderstood as device management. There is an enormous volume of industry discussion on this topic, but the issue only gets more confusing when you consider the huge number of IoT devices being deployed and the variety of functionality, environments, and use cases involved. This often leaves product engineers with more questions than answers on an issue that has far-reaching impact on the design, deployment and operation of IoT devices. Device management is critical to the long-term success of any IoT deployment.

It is important to separate the topic of device management from discussions of a related but different topic: telemetry. Telemetry is the stream of business-related time-series data that comes from IoT devices such as sensors and other equipment – which organizations rely on to gain actionable insights for their operations. This data is often the basis for digital products and services where reliability is key. Ensuring reliable telemetry delivery is a primary goal of every IoT deployment, and effective device management is the means to achieving that goal. Without the right device management strategy during IoT device design, companies will not reliably get the data streams they have invested so much to obtain.

vs. embedded IoT device management needs, the issue becomes less and less clear to product engineers looking for practical advice on the subject.

When seeking solutions for device management, marketing language often compounds this confusion. Many solution providers are recognizing the importance of device management, seeing it as a growth market where they can make quick sales if they list the right features or buzzwords. This flood of sales pitches makes already-muddy waters far muddier. After all, if two companies selling dramatically different technologies that tackle completely separate aspects of



One major contributing factor to confusion around device management is the difficulty of defining what exactly "device management" means. The author of the article you read yesterday about device management may be discussing its use in a very different context than the company that is promoting its device management platform at the event you attend next week. So often, companies are talking about different things entirely but use similar language, making it difficult to apply to your own solution. It's not always an apples-to-apples discussion due to the variety of needs from IoT operations and use cases.

"Device Management" is also used differently across disciplines, often meaning different things depending on what type of devices are involved. Managing devices like corporate workstations, smartphones, and tablets is fundamentally different from device management of headless, low-power embedded IoT devices running purpose-built software stacks. Industry discussions often treat device management as a one-size-fits-all topic relevant to all connected devices. With so little distinction between traditional IT/DevOps

remote device management both use identical marketing language with identical lists of customer benefits, who can tell the difference? It is no surprise this topic is challenging for product engineers to navigate.

It would be tempting to just shrug and ignore the muddy mess until the industry gets itself on the same page. After all, sometimes it takes a while for members of the tech industry to build consensus on an issue and start speaking the same language. The early days of IoT have plenty of examples of exactly that as consensus slowly emerges on standards and best practices. But in the case

of device management, waiting for the fog to fully clear is not a practical option. Not having the right device management strategy today will inevitably lead to significant problems in the future once your IoT device network is deployed.

Device management problems typically only rear their head after IoT devices have been designed and deployed in the field for a period of time. The result is an ambush of requests to the support and engineering teams to quickly deliver embedded software updates, security patches, or add new functionality to devices they typically no longer have easy access to. In these situations, engineering teams learn too late that devices are designed or provisioned in ways that make these kinds of remote updates difficult or impossible to do at scale. This results in the need to roll trucks to solve the problem either with more infrastructure investments or with manual updates – both of which are costly, time-consuming, and a shock to organizations who thought these bases were already covered. In these situations, manual updates are often the only solution – requiring technicians to visit each device, remove housings, plug into the device using special equipment, and make updates to the embedded software. This isn't the exception, it's the rule if IoT devices being deployed do not have a device management system designed in right from the start.

Even worse than manually rolling out updates are device management problems that engineering teams are completely unprepared for or unaware of. Networks and devices go down. It's a frustrating fact of life for IoT deployments, and it necessitates rapid responses in order to restore network functions and data flows. But what if teams have no way to gather insights about where those outages are happening, how long they have been going on and whether data streams are offline? Once again, this is not an unlikely worst-case scenario. This is frustratingly common because device and connectivity health reporting capabilities in so many IoT networks have blind spots, allowing small incidents like device connectivity issues to snowball leading to costly down time and poor quality of service for upstream digital products relying on these data streams.

This white paper provides a game plan for avoiding many frustrating, costly device management problems as discussed above. Below are four pillars for an effective device management strategy that your team should factor into the earliest stages of an IoT project, ensuring that you are not ambushed by device management problems after devices are activated in the field.

Automated Device Provisioning and Deployment Approach

Successful IoT deployments start with a solid device provisioning process, properly identifying and configuring the device to operate within a larger system. These provisioning steps can sow the seeds of future device management problems if not designed properly. The focus is often on speed-to-market and how the device will support telemetry-driven use cases rather than ongoing device management operations. Unfortunately, the importance of these ongoing device management requirements will often not become clear until later in the product life cycle when it is too late to add such features.

Engineering and manufacturing teams should review their provisioning process and consider implications to supporting device management operations. Best practices for this include:

- **Registration of each product during manufacturing stages**

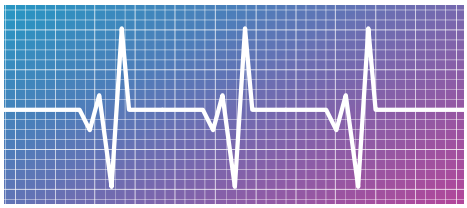
to reduce touch time at installation

- **Automated connection to the device management system once connectivity is established**
- **Ensuring device connectivity status can be remotely monitored and diagnosed post-deployment**
- **Features to remotely report software versions and securely deploy software updates**
- **Capability for remote review, verification, and update of device operational parameters**
- **Remote provisioning updates, including device management and telemetry service credentials**

The most common mistakes I see with this pillar of device management are:

- **Lack of automated provisioning process leading to costly manual setup steps at device installation**
- **Weak or no support for remote firmware updates leading to costly manual update procedures**
- **Under-developed connectivity monitoring strategy leading to down-time and telemetry data loss**
- **No planning for credential rotation or dealing with IoT device certificate expiration leading to sudden loss of connectivity with no approach to recovery without a site visit from a technician**

A provisioning and deployment process shaped by a forward-looking device management strategy will help you avoid these pitfalls.



Real-Time Device Health Monitoring

Every IoT device engineering team puts a focus on data reporting, but too often the focus is on telemetry data without enough focus on the data and functionality required to support effective device management. As discussed at the beginning of this white paper, the confusion between the value of telemetry vs. device management can cause an imbalance of focus, leading to potential blind spots and failure modes that are difficult to troubleshoot once a fleet of devices is deployed in the field.

Engineering teams should therefore ensure that they put as much focus on remote access to device operational and connectivity health data as they do on telemetry data, including:

- **Real-time status of signal strength and other connectivity metrics to gauge network health**
- **Access to device system logs and diagnostics data to assist troubleshooting of connectivity issues**
- **Operational status (e.g., battery levels) and other metrics related to ensuring device up-time**
- **Proactive configuration of alerts to report emerging device health or connectivity issues**
- **Interoperability with device management software services to monitor and manage devices at scale**

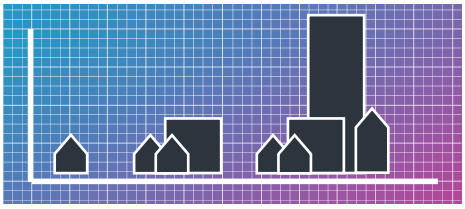
The biggest trap engineering teams fall into is mistakenly assuming device health monitoring functionality is already built into the embedded software of their devices. In practice, unless device-side features are matched with coordinated cloud services for monitoring and alerts, they aren't very useful in practice for detecting issues. Health monitoring features designed for an individual device or pilot project do not necessarily scale up to what is needed once hundreds or thousands of devices are deployed.

Failure to plan for scalable device health monitoring leads to:

- **Lack of alerts for device health related conditions**

operators should be aware of

- **Lack of diagnostic insights into cause of operational breakdowns or interruption of telemetry data**
- **Lack of visibility into issues that can interrupt real-time data transfer critical to many use cases**
- **Lack of detection of emerging issues (low batteries, software bugs, etc.), leading to the need for emergency actions to bring systems back online**
- **Difficulty collecting health data and recognizing performance issues in large-scale deployments**
- **Difficulty isolating where an issue resides within the system during troubleshooting/maintenance**



Path to Scalability

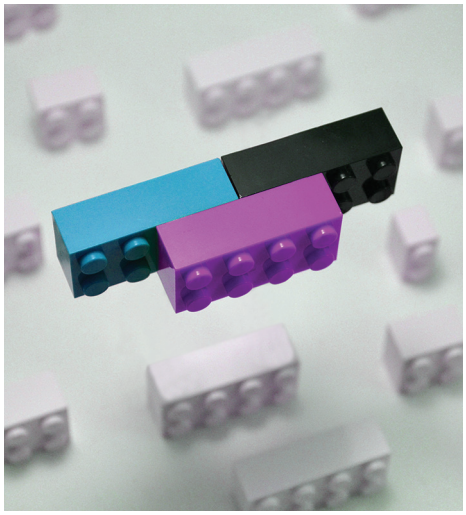
As mentioned, a successful device management strategy drives the outcome of a scalable IoT solution. Scalability needs to be at the heart of an organization's device management strategy since many of the problems discussed throughout this white paper multiply in intensity at scale. An obvious example when planning for scale is how to support remote software update of fielded IoT devices. For pilot projects, engineering teams can often meet this need by using a mobile app to send software updates over the air to a device they are standing next to using a technology such as Bluetooth Low Energy. Though convenient, this approach does not scale well when you have large numbers of devices across a variety of sites and often installed in hard-to-reach locations such as above ceiling panels or mounted to remote equipment.

Engineering teams need to ensure their sensors and gateways are designed for a smooth path from small-scale to large-scale device management. Remote updates for any kind of IoT device are challenging, but low-power wireless embedded IoT devices amplify such challenges due to their limited resources. These devices often require RTOS, device management, telemetry and application software to be built into a single package and therefore require planning for system integration and scalability right from the start.

To ensure scalability, your device management strategy should enable:

- **Robust remote software update procedures, providing a path to security updates and bug fixes for devices in the field arising well after the initial launch of your product**
- **The ability to review and update operational parameters for devices in the field**
- **The ability to verify and update credentials for device management and telemetry services**
- **API-based access to devices enabling automation and integration into cloud applications**
- **Automation of software maintenance functions including version reporting, diagnostic reporting, commissioning, and decommissioning procedures**
- **Access to system logs to aid in identifying events leading up to connectivity or data loss issues**

Scalability is the pillar that is most often overlooked by engineering teams in early IoT product planning. Without a path to scalability, the perceived value and success of pilot projects will not be replicated as the number of devices increases and variety of installation environments expand. Factors related to scalability include: lack of support for remote software or firmware updates, lack of support for remote configuration updates, lack of visibility into root cause of connectivity or other failure modes, and inability to bring telemetry data streams back online after a breakdown in connectivity without an on-site visit.



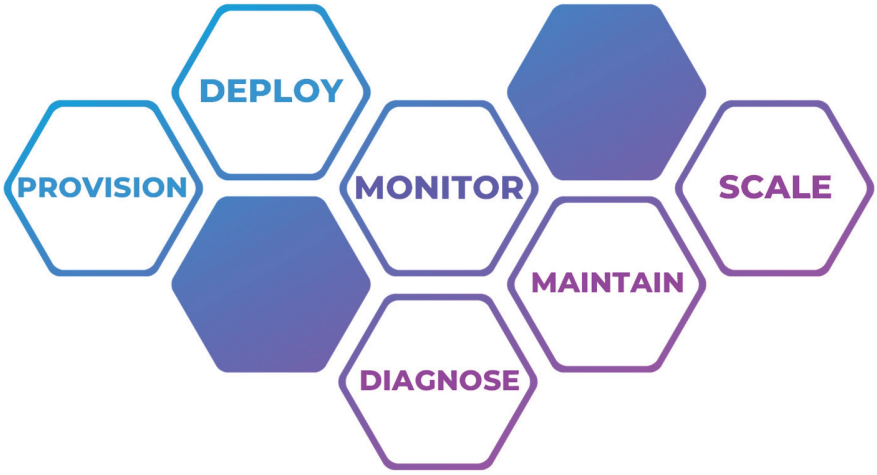
Flexibility in Application Development

As I mentioned in the introduction of this white paper, device management is about being prepared for the long-term – the future when devices are in the field, long after they start streaming telemetry data and providing initial return on an organization's investment in IoT. This final pillar addresses one of the most important

aspects of future-proofing your organization's investment in IoT: ensuring that devices in the field will successfully live their full life cycle even as technology trends evolve over the course of years.

A successful device management strategy can futureproof IoT projects by:

- **Using standards-based protocols reducing vendor lock-in and avoiding outdated technologies**
- **Utilizing embedded architecture that accommodates firmware requirements changing over time**
- **Reducing dependency on technologies that require specialized engineering, training, and support that may be in short supply in the future**
- **Establishing partner and software ecosystems to keep pace with ever-changing software, security, and system requirements beyond your control**
- **A simplified path to customizing application firmware to deliver new functionality over time**
- **Automated processes for ensuring device configuration remains compliant over time**
- **A strategy for addressing security issues over the lifetime of the device**



Without this final pillar, organizations risk the premature obsolescence of their IoT deployments or the need for costly manual upgrades by rolling trucks for massive, expensive on-site rescue operations.

A device management strategy built on these four pillars will provide a solid foundation for large-scale IoT deployments that are successful both in the short term and in the long term. Laird Connectivity has worked with many organizations to simplify IoT design and deployment by enabling effective device management and telemetry solutions. See below for information about our new device management platform, Canvas™ Device Manager, which provides a simplified path to address each of the device management needs discussed in this white paper.

About Laird Connectivity's Device Management Solutions:

Canvas™ Device Manager is Laird Connectivity's new device management platform that simplifies workflows for configuration, monitoring, and maintenance of IoT device deployments. This platform provides low/no touch device setup, device health monitoring, and other device management focused features to keep your entire IoT device fleet online. Canvas Device Manager allows you to configure telemetry data streams to the application cloud platform of your choice. Rapidly respond to constantly evolving security attacks and keep your devices safe and compliant via the remote software and configuration update features of the platform. Keep your IoT-driven services and revenue streams online by providing your operations team powerful tools for scalable device management.

Laird Connectivity has partnered with EdgeIQ and other industry leading cloud-based and SaaS providers so that customers do not need to integrate multiple 3rd party components themselves. Canvas Device Manager cuts ownership costs with an option for pre-provisioned devices, enabling rapid scale up of IoT solutions.

CANVAS™
DEVICE MANAGER

For more information about Laird Connectivity's Canvas Device Manager, visit:

https://www.lairdconnect.com/iot-devices/canvas-device-manager

About the Author

Scott Lederer is Engineering Manager at Laird Connectivity, which simplifies wireless connectivity with market-leading RF modules, internal antennas, IoT devices, and custom wireless solutions. Scott has 20 years of product-focused software development and leadership experience with cross-disciplinary teams delivering solutions across several industries. He has worked the last five years managing a software engineering group within Laird Connectivity's Engineering Services division focused on IoT product development including solutions for simplifying IoT device management and telemetry. Laird Connectivity's multi-disciplinary design services team provides all aspects of development for the latest cloud-connected products, from prototype through manufacturing. Scott holds a Bachelor of Science degree in Computer Science from the University of Wisconsin–Madison.

About Laird Connectivity

Laird Connectivity simplifies wireless connectivity with market-leading RF modules, internal antennas, IoT devices, and custom wireless solutions. Our products are trusted by companies around the world for their wireless performance and reliability. With best-in-class support and comprehensive product development services, we reduce your risk and improve your time-to-market. When you need unmatched wireless performance to connect your applications with security and confidence, Laird Connectivity Delivers – No Matter What.

Learn more at [www.lairdconnect.com.](http://www.lairdconnect.com)

Laird™

CONNECTIVITY