Brought to you by:

arm

IoT Solutions

for dummies®

A Wiley Brand

Design a robust, scalable IoT solution

Manage deployment

Stay secure and connected

Lawrence C. Miller

Arm Special Edition

About Arm

Arm defines the pervasive computing that shapes today's connected world. Realized in 110 billion silicon chips, Arm's device architectures orchestrate the performance of the technology transforming our lives—from smartphones to supercomputers, from medical instruments to agricultural sensors, and from base stations to servers. Every day thousands of Arm partners embed more than 45 million Arm-based chips in products that connect people and enhance the human experience, to serve today and architect tomorrow.

To discover more, please visit Arm.com.

IoT Solutions

Arm Special Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

IoT Solutions For Dummies®, Arm Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-50335-4 (pbk); ISBN 978-1-119-50336-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Senior Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Siddique Shaik

Introduction

The Internet of Things (IoT) will create a global network of connected and intelligent devices that will inform and enhance society and business. Many important challenges and design considerations, such as regulatory requirements and post-deployment management of IoT devices, must be addressed early to build a complete and secure IoT solution.

About This Book

In this book, you'll learn what is required to design a robust and scalable IoT solution serving a range of markets and needs, including important challenges to consider and why it is vital to address those challenges at the earliest stages of planning and design.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless! I assume you work for a company that is interested in building an IoT solution to support the delivery of data-driven services for your customers, or for optimizing your own processes and assets. Perhaps you're a CIO or the director of an engineering team responsible for key

decisions related to the planning and design of your IoT solution. As such, I assume some technical knowledge and familiarity with IoT enabling technologies. If any of these assumptions describes you, then this book is for you!

Icons Used in This Book

Throughout this book, I occasionally use icons to call out important information. Here's what to expect.

REMEMBER

This icon points out information you should commit to your nonvolatile memory.

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

TIP

Tips are always appreciated, never expected. I hope you'll appreciate these useful nuggets of information.

WARNING

This icon points out the stuff your mother warned you about (well, probably not). But these helpful alerts do offer practical advice.

Beyond the Book

There's only so much I can cover in this short book, so if you want to learn more, just go to `www.arm.com`.

IN THIS CHAPTER

- Explaining the Internet of Things
- Leveraging a complete IoT ecosystem

Chapter 1
The IoT's Business Implications

In this chapter, you learn about the Internet of Things (IoT): what it is, what opportunities and challenges it presents, and why a complete innovation ecosystem is critical for success.

Defining the IoT

The IoT is a network of *physical* objects (such as wearable devices, home appliances, security systems, personal and commercial vehicles, nanotechnology, manufacturing

equipment, and more) embedded with *smart* components (such as microprocessors, data storage, software, sensors, actuators, and more) and *connected* to other devices and systems over the Internet.

At the micro scale, the "thing" may be an individual component, such as a smart lighting unit in a commercial office building, or the building itself, as an item in a portfolio of assets being tracked.

The value of the IoT is in the data that is collected and then analyzed to provide insights or actions. To ensure the integrity of that data, the whole system must be secure and managed.

A vital part of that is the choice of connectivity protocol. The sustainability of the system depends upon being able to reliably transmit data over a variety of distances and through a broad array of materials, in the most energy-efficient way possible. The efficiency element is critical because many, perhaps most, IoT applications will depend on battery-powered sensors — whether that sensor embedded is in an electric vehicle, buried in a farmer's crops, or installed inside a bridge or building.

REMEMBER

IoT devices may collect, store, and share data and/or perform advanced control functions — such as smart meters and light bulbs, autonomous self-driving vehicles, and sophisticated industrial equipment — increasingly using artificial intelligence (AI) and machine learning (ML).

Looking at the IoT's Rise

Over the past year, a major transformation in how businesses view the IoT has occurred. A recent Economist Intelligence Unit (EIU) IoT Business Index surveyed executives and senior business leaders from around the world. Fifty percent reported that IoT was an important part of their business strategy and that many of those companies were already rolling out IoT services.

By 2022, the combined Industrial Internet of Things (IIoT) market in North America and Europe is expected to be worth more than $1.2 trillion, with a compound annual growth rate (CAGR) through 2021 of 13.1 percent and 11.9 percent, respectively, according to Mind Commerce.

Avoiding Potential IoT Pitfalls

As with any rapidly evolving opportunity, significant challenges must be addressed in the IoT market. Perhaps the biggest pitfall to avoid is failing to define a commercially viable business model. You need to clearly define the use case and capture the business requirements for the problem being addressed — for example, providing a service, product lifecycle engineering, customer satisfaction, or operational efficiency improvement — and align all your efforts toward solving that problem.

WARNING

An IoT system designed without the customer at the center is frequently doomed to fail.

Another common pitfall for large and even medium-size organizations is failing to adequately navigate the digital transformation an organization must go through if it is to capture the benefits of IoT, especially at scale. It is important to have a plan across divisions and/or functional groups. Pitfalls to be addressed include:

- **Scalability and efficiency:** Building any network requires careful consideration and design flexibility to achieve scale. This ranges from the type of devices and network designs employed for particular use cases to the broader question of whether the industry has the right engineering resources to attack the problem (see Chapter 2).
- **Management and connectivity:** The technology industry has traditionally been divided into hardware and software solutions, with one side throwing a solution over to the other to complete the system. But to scale IoT, hardware and software must be considered and implemented up front because the long-term resiliency and usefulness of an IoT solution must be constantly managed and optimized (see Chapter 3).
- **Security and social responsibility:** Cybercrime costs the global economy one-half trillion dollars a year in economic losses, ransom payments, and dealing with

the resulting chaos. While the advantages of what a connected world can do for people and businesses still vastly outweigh the threat, businesses must ensure that they can maintain trust in the system. To do this, business must act collectively and accept that all technology companies share the responsibility to deliver collectively on the promise of secure devices and systems (see Chapter 4).

Recognizing the Need for an IoT Ecosystem

The IoT market is characterized by the rapid development of new products, software, and technologies. In this fast-paced environment, industry standards and government regulations can be outdated, because they typically fall behind the breakneck speed of innovation for the world of tomorrow. Thus, technology vendors must be proactive in their efforts to ensure interoperability with other technology vendors in the IoT ecosystem, improving communications and transparency around cyberattacks and exploits, to ensure effective security.

REMEMBER

Scaling to billions of devices means that technology and people must work together. From cloud software to connected sensors, your IoT ecosystem must provide the solutions you need.

Examples of services and the value proposition in a robust partner ecosystem include design services, such as system on chip (SoC) design, software integration, and hardware customization, as well as these support services:

- **Training**
  - *Reduce risk* (equip engineers with the knowledge they need)
  - *Accelerate time-to-market* (allow engineers to start designing sooner)
  - *Increase team motivation* (improve confidence in design)
- **Design reviews**
  - *Reduce risk* (identify design issues while they can still be easily fixed)
  - *Improve success* (avoid flaws that could limit the functionality of your product)
  - *Expert review* (get assistance at key stages throughout your design)
- **Technical support**
  - *Comprehensive documentation* (easily accessible online product information and resources)
  - *Fast resolution* (expert assistance to resolve technical issues quickly)

IN THIS CHAPTER

- Starting with IoT platform requirements
- Evaluating design choices
- Looking at hardware

Chapter 2
Building a Scalable and Efficient IoT

In this chapter, you learn about the basic requirements for IoT devices, IoT deployment options and design choices, plus different IoT platform hardware approaches.

Defining Your Requirements

In the race to the "next big thing" for the Internet of Things (IoT), businesses must define their unique

technical requirements. However, there are four crucial requirements for the IoT in general:

- **It needs to work separately.** The different components of an IoT solution must be able to function independently, and be managed independently, as well as a part of the whole. Individual components may need to be periodically replaced and cannot interrupt or reduce the functionality and effectiveness of the hive of devices.
- **It needs to work together.** For the promise of IoT scale to be realized, the "things" must add more as a whole than as individual components; otherwise the return on investment (ROI) for connecting them in an IoT solution is reduced. They must communicate with each other and with the cloud to make the best and most efficient use of collected data.
- **It needs to leverage automation.** Machine learning (ML), as an enabler of artificial intelligence (AI), will play an increasingly important role in IoT devices. A case in point is image recognition, in which a system can be trained to determine, with a high degree of confidence, whether it's looking at different objects such as a child or a cat. Currently, most of these systems rely on data being transmitted to the cloud. But, some image recognition is simple enough that it can easily be handled in the camera itself. This capability reduces latency and

communications bandwidth while improving user privacy in some cases. In the future, ML will become more distributed with functionality available at the edge of the device network. This will allow both learning and training at the edge, so devices will have ML capability independent of the cloud. Again, this will improve latency and be more secure.

- **It needs to work resiliently, securely, and safely.** Security requires heightened focus from the edge to the cloud to protect against both known and unknown threats. Part of this is to make end-users do much less of the work in the security chain, and make it invisible for them as part of their daily routines. Connected IoT devices must also work reliably and operate safely.

Exploring Your Options

The deployment of IoT devices at scale requires flexibility, coverage across a vast range of IoT client devices, and communications efficiency — irrespective of device constraints. With easy integration and increased developer productivity, enterprises can rapidly roll out and manage full-scale deployments. Cloud-based device management services can simplify the connecting, securing, provisioning, and updating of any devices across complex networks.

Connecting the old

Developing a business case for an IoT deployment will be different depending on the level of "connectedness" already in a system, as well as the amount that will be required in the future.

A number of companies already have some sort of tracking or sensor-based regime in place; in particular those operating in sectors such as commercial buildings, goods transportation and utilities. However, companies' current technologies may not allow for individual tracking — that is, individual IP addresses for each sensor. Upgrading to a full-scale IoT system would provide a major improvement in the value they can get from data, in terms of quality, quantity, and what the data can be used to do.

In this case, a way of linking from the existing device data network to a gateway that allows full remote management via the Internet is required. Systems with this capability are now becoming available.

In addition, many companies — including those using cloud-based solutions in other areas of their enterprises, require on-premises IoT solutions. This allows them to retain full control of device management systems and data. It is a key demand in sectors such as utilities because cloud sharing of sensitive data, now isolated behind firewalls or going to a local data center, is not an acceptable risk.

Connecting the new

Whether you are looking to connect an intermediary device to "passport" data from an old network to a new one, or are building a new system using advanced digital sensors (32-bit/64-bit) from the start, you need to consider how devices will be managed.

Today's increasingly complex IoT use cases strongly benefit from endpoint devices that leverage an embedded operating system (OS) that brings a comprehensive suite of security and connectivity elements. These elements make the creation and deployment of IoT solutions at scale a reality.

TECHNICAL STUFF

Although having an OS is not mandatory, IoT devices are growing in complexity due to nodes having more sensors, data processing, and connectivity to send data. End devices that were often based on 8-bit or 16-bit microcontroller units (MCUs) are moving to 32-bit architectures as costs drop and complexity increases. Addressing these changes without an OS is not only a challenge but also inefficient. The use of an OS, in particular a real-time OS, simplifies the job of application programmers and system integrators because many of the low-level challenges are taken care of by the OS.

Some important OS characteristics include:

- **Modular:** Necessary libraries are included automatically on your device, allowing you to concentrate on writing application code.
- **Secure:** Multilayer security protects your IoT solution, including isolated security domains, secure over-the-air (OTA) updates, and Transport Layer Security (TLS) for secure communications.
- **Connected:** Support for a wide range of connectivity options with drivers for communications protocols and technologies such as:
  - Ethernet and Wi-Fi
  - Cellular, including 3G, 4G Long-Term Evolution (LTE), LTE Advanced, LTE Advanced Pro, 5G (in development), and NarrowBand Internet of Things (NB-IoT)
  - Bluetooth classic
  - Low-power alternatives, including Bluetooth low energy (LE), Bluetooth mesh, IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), Long Range (LoRa) LPWAN, Thread, ZigBee, and others
  - Near-field communication (NFC) and Radio-frequency identification (RFID)

Considering Different Hardware Approaches

IoT use cases vary in the extreme. They can be simple sensor devices existing for ten years or more on a coin cell battery and transmitting "tiny data" periodically over long distances (such as in a field or on an oil rig). They can be RFID "smart tags" tracking goods on pallets. They can even be embedded building sensors that may be mains-powered.

The key in the vast majority of applications is energy efficiency. Important considerations that affect energy efficiency include:

- Energy profile
- MCU/CPU security (basic to strong)
- Connectivity protocol (distance, power, security)

The reality is that most IoT devices will not be mains-powered, so the main IoT chip must use a highly efficient architecture. This can be off-the-shelf or if design resources allow, a custom system on chip (SoC) based on standard IP components.

Off-the-shelf requires a vast choice of products so that your design is scalable. Many IoT devices will evolve as the value of collecting data increases and the product

needs greater compute power. You need access to a menu of performance options and the ability to tie into other intellectual property (IP), such as digital signal processors (DSPs) to bring all your sensors together (sensor fusion).

Some architectural companies offer low-risk ways to work up a custom SoC prototype, so that developers can get to scale before thinking about upfront paid licenses and royalties, which are success-based.

Whether you choose off-the-shelf or custom SoC, either choice will require:

- Easy access to design tools
- Approved design houses if you don't have in-house expertise
- An established and expansive software ecosystem (experienced in working with your chosen chip architecture)
- Foundry partners equipped with relevant performance optimization pack (POP) IP to manufacture your chip in the most effective way possible

IN THIS CHAPTER

- Deploying device updates
- Rolling out security patches
- Scaling to thousands of devices
- Staying connected

Chapter 3
Managing IoT Deployments

In this chapter, you learn about updating devices in the field, patching security vulnerabilities, managing thousands of IoT devices at scale, addressing legacy and on-premises systems, and maintaining connectivity in diverse and challenging operating environments.

Updating Devices

One of the major challenges facing IoT deployment is addressing the operational needs of devices throughout

their life cycle, particularly in ensuring that devices have the correct software installed, that firmware is protected against security vulnerabilities, and that application and functionality updates are managed.

IoT devices typically have a product lifetime of 20 or more years. Over the lifetime of a product, there is a need to unlock additional business potential, address functional defects, and manage constantly evolving securing challenges. Remote over-the-air (OTA) software updates are the most efficient way to distribute and install required software changes.

Key requirements for updating IoT devices include:

- **Secure:** The authenticity and integrity of updates should be verifiable.
- **Fail-safe:** Update campaigns should be protected during power failures.
- **Campaign tracking:** Accurate campaign tracking reduces maintenance costs.
- **Conditional control:** Business rules should prevent interruption of critical device operations.

To efficiently update IoT device applications at massive scale, technology vendors must leverage the cloud. Vendors should create a trusted chain between device and cloud, with trust anchored at both ends. This means that the device network must also be secured by a root of trust.

In so doing, trust is "baked" into the device and moves closer to the edge of the network. By enabling automatic device updates, rather than physically visiting devices, there are also potentially huge cost savings to be realized.

TIP

Lower costs are realized by reducing field call-outs for devices that haven't updated as desired in the campaign. Being able to remotely troubleshoot devices from afar can save hundreds, if not thousands, of dollars each time someone has to be sent into the field to access devices.

Security must be a cornerstone of any cloud-based update delivery service. The service must ensure secure delivery of authenticated and validated firmware to secure devices over multiple infrastructures and protocols that are essential for connected industrial operations. Because security elements are independent of transport protocol, the service must support a wide range of protocols. It should also support caching in the cloud environment. This feature enables users to bring update capability across a range of networks while saving money and improving flexibility. The service should also support encrypted update packages to protect intellectual property (IP) or to observe security licensing restrictions.

Further, updates across large deployments scaling millions or billions of devices can take a long time. Thunderstorms may not always be the culprit, but power fluctuations or power outages during long update

campaigns are all too common. Your update service requires proper software/hardware design and should support practical considerations for remote throttling and rollback protection, preventing devices from being accidentally or maliciously rolled back to an older, more vulnerable firmware version.

WARNING

Factory and default settings on a device are popular targets for rollback attacks. You also need to ensure that your firmware and software updates don't restore any factory or default settings that may inadvertently make a previously secure device vulnerable.

Patching and Securing IoT Devices

Similar to the challenge of updating applications, the ability to quickly deploy security updates is necessary to ensure IoT devices operate securely and safely.

Security updates are typically smaller in size than application updates, but must occur more frequently — and often quickly to reduce exposure time when a new vulnerability is discovered.

Original equipment manufacturers (OEMs) typically ensure that security updates are delivered or made available to device owners and operators in the field.

Additionally, technology vendors and customers must be able to prove that security patches were properly installed, for regulatory compliance and due diligence purposes, with secure audit and logging capabilities.

Ensuring Scalability

Deploying application updates, security patches, and remotely managing the operation and maintenance of many thousands of devices requires massive scalability and flexibility. For example, industrial and enterprise customers might need to leverage a system that delivers a consistent security model across gateway, on-premises, and private and public cloud environments.

By leveraging the cloud, some of these functions may be moved closer to the customer's edge network to provide compute, storage, and network resources that deliver the robust and scalable architecture required for a successful IoT deployment.

At the same time, it's important have the choice to keep solutions on-premises, because many companies are loath to transition their legacy systems into the cloud, where their valuable data might be exposed.

Remotely connecting to a device helps technicians to quickly troubleshoot device or application issues, or train end-users in the operation of devices and applications.

Remote troubleshooting helps to correctly identify the root cause of an issue, so the right parts and/or field technician can be sent to the customer on the first trip.

Maintaining Connectivity

In the industrial context, a remote device may be embedded in a harsh environment where access is limited. It may be buried next to a mast in a weatherproof case, and it may require technicians to travel hundreds of miles to repair. These devices may be deployed across a diverse network topology. Mechanisms designed for previous networked equipment may even be too constrained for IoT devices.

When considering the needs of teams responsible for managing and updating IoT devices, the success and return on investment (ROI) of IoT deployments depends on addressing questions like:

- How can I update my devices?
- What happens if a thunderstorm hits?
- What if a power outage during the update corrupts information on the device?

Support for a wide array of communications technologies and protocols is essential for maintaining connectivity under such challenging conditions.

IN THIS CHAPTER

- Addressing IoT security needs
- Building and maintaining trust

Chapter 4
Exploring Security and the Digital Social Contract

A battle is raging to keep systems secure as the world races to realize the immense value of the Internet of Things (IoT). As part of this battle, technology companies have a responsibility to society extending beyond just delivering products.

In this chapter, you learn why IoT resiliency and security risks must be addressed with greater urgency, and with a new approach by end-users and technology providers.

This chapter also explores why a "Digital Social Contract for Security" is critical to building and maintaining a foundation of trust for the IoT.

Addressing Security

We are witnessing cyberattacks on critical infrastructure, health services systems being held for ransom, and home electronics devices used as Internet gateways by hackers. The result, according to Lloyd's of London, is that cybercrime might be costing the global economy a half-trillion dollars a year because system and device security across all sectors are vulnerable to new attack methods.

The challenge of keeping systems secure has become a primary design consideration for the major technology companies. However, the risks to a system do not only lie with the hardware or software. Increasingly, cybercriminals are looking to circumnavigate built-in security through relatively simple social engineering techniques targeted at exploiting human vulnerabilities. Users are often the weakest link in secure systems.

As the interface between technology and human users becomes less distinct, and as the threats to personal safety become greater (for example, a hacked home security system that could be used to invade occupants' privacy), users must be their own first line of defense. This is true at a personal level as cybercriminals will continue to perpetrate identity theft and credit card fraud for the

foreseeable future. It becomes even more important at the global level as cyberterrorists, competing nations, and hacktivists are likely to exploit the IoT to commit destructive and potentially lethal cyberattacks.

REMEMBER

Technology providers must embrace their own responsibilities with a "Digital Social Contract for Security" and endeavor to protect users — despite themselves — to create a foundation of trust.

Keeping a Social Contract

All technology companies' responsibilities under the Digital Social Contract are rising as connected devices proliferate. Cyber attackers are becoming increasingly sophisticated, so technology companies must continue to push security as a primary design consideration, ensuring that security defense scales with the threat. This Digital Social Contract will then form a foundation for explicit trust between the technology sector and all users.

Adherence to the Digital Social Contract will require companies to go well beyond the legal language in their terms and conditions, and regard robust security as a prerequisite in all design decisions. It will mean taking full account of how people are likely to use their technology, not how companies would like them to use it.

Although the Digital Social Contract also places a duty of care on users to protect themselves by behaving

responsibly, technology designers will always carry the major burden because most end-users are not technology or security experts. It will require a swift departure from the mindset in which companies consider it acceptable, for example, to ship products with device passwords as simple as `12345` or `PASSWORD`.

The challenges in honoring the Digital Social Contract vary according to the area companies operate in. For example, the automotive industry is a 100-year-old sector going through immense disruption with the move to mass electric and hybrid fleets and fully autonomous self-driving vehicles.

Traditionally, automotive companies take seven to ten years to move from design to delivery. Today that innovation cycle is shrinking as they face competition from technology companies used to taking products to market much faster. It may be thought there is a possible risk that the Digital Social Contract could be damaged by such a disrupted competitive landscape. However, the automotive industry is governed by functional safety standards ensuring that vehicles meet stringent safety targets. In this case, the Digital Social Contract is underpinned by a legal duty of care. So, while automakers are working out how to go faster, competitor technology companies are learning how to operate in a more highly regulated safety environment.

The risk to the Digital Social Contract is higher where time-to-market pressure is greatest. Security risks affect

all markets but are potentially the most damaging in business markets and critical infrastructure because the fallout from an attack is likely to be higher.

Evidence of this growing threat came from the U.S. Department of Energy when it warned that electricity systems faced "imminent danger" from cyberattacks and threats were increasing in "sophistication, magnitude, and frequency." Also, in 2017, the UK's National Cybersecurity Centre reported around 600 "significant" attacks over the last year and thousands prevented.

As connected technologies scale, technology companies must reset their thinking. In fast time-to-market segments, success is built on the model "design, ship, analyze, and pivot" — in other words, learning fast and iterating. But this approach can undermine robust security because weaknesses in products once they are deployed are harder to correct. Changing this model can be difficult in design-fast, iterate-fast markets where there might be a perception that best-practice security can affect schedule and the bottom line.

The way to change that perception, especially in a hot market like the IoT, is to remember that security is good for the bottom line and embracing a new, more resilient business model doesn't hurt time-to-market. This change will be possible by making secure-by-design technologies readily available to developers. This will enable a new business model built for the IoT, one that aligns perfectly with Social Contract responsibilities.

The new model will make it harder to breach chip security and allow more time for system defenses to react. This model can be summarized as:

- Design for security
- Ship
- Analyze
- Self-heal or quarantine
- Treat (if required)

This model will be crucial in segments like the IoT with the potential for vast numbers of deployed, connected devices in a single system. It will provide a more complex model protecting system integrity, and ensure the technology sector takes life cycle responsibility for products.

This model covers the ability to patch devices en masse, such as with smartphone bug fixes. The evolution will also bring the capability to manage individual devices in a surgical manner. This will enable the quarantine of single devices until they can be rehabilitated.

REMEMBER

The key to this new business model is distributed intelligence. It means pushing the kind of powerful compute capability now found mainly in the cloud to the edge of the device network. This will move organizations from rigid command-and-control structures to a more flexible, dispersed security model.

IN THIS CHAPTER

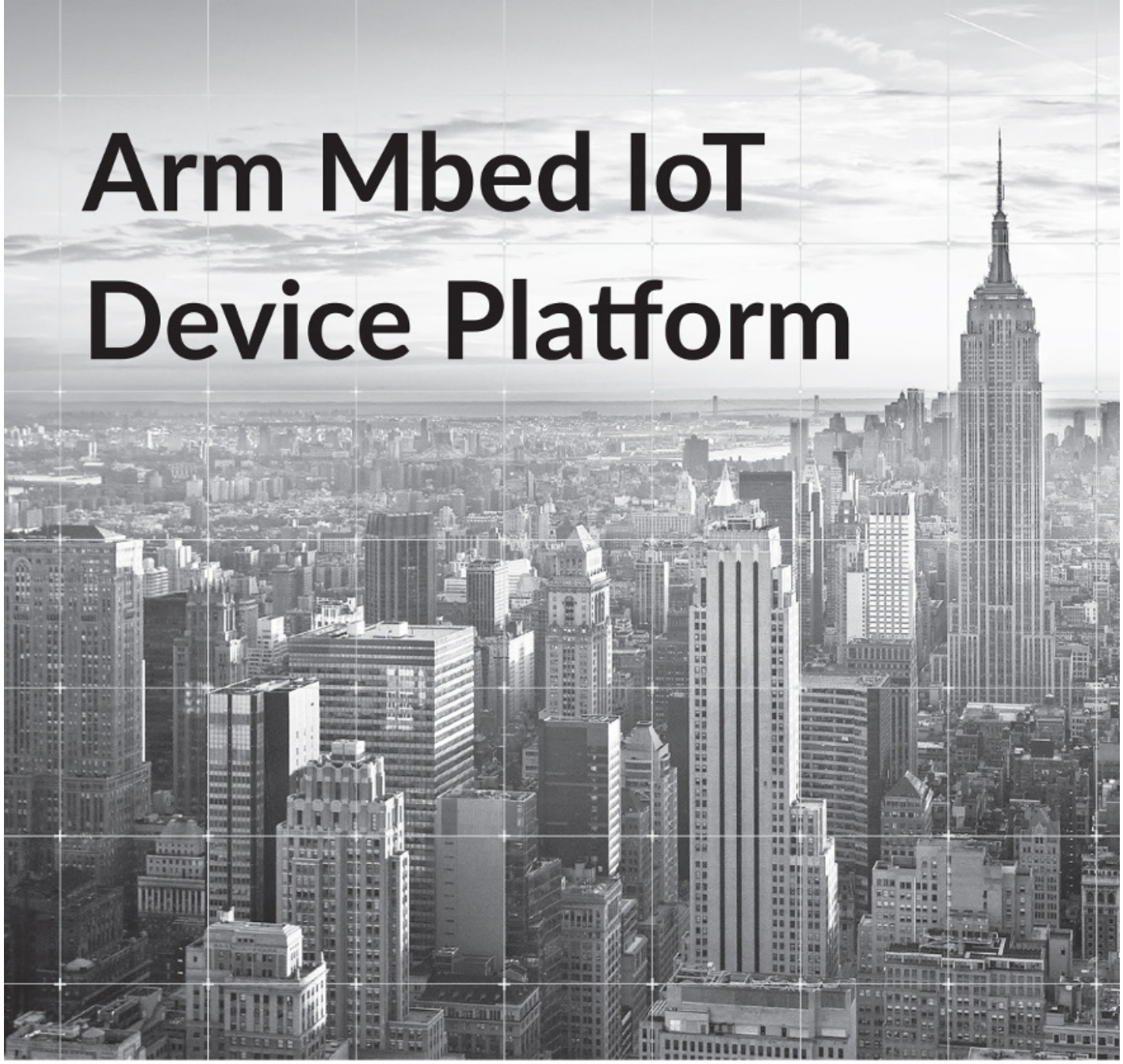
- Managing and updating at scale
- Staying connected
- "Future-proofing" your solution
- Improving security

Chapter 5
Ten Principles of a Successful IoT Deployment

This chapter provides ten key principles to help you design a successful IoT solution:

- Ensure post-deployment management and maintenance capabilities at massive scale, and define a complete deployment-to-obsolescence device lifecycle management plan.

- Plan and design for robust connectivity in harsh, isolated operating environments, and define resilience and safety requirements.
- One size does not fit all. Power (battery life), size, and reliability are crucial in IoT systems.
- Leverage a proven ecosystem for flexibility and choice, and to help "future-proof" your solution.
- Identify a robust commercial business plan, including building a complete use case for how you plan to leverage the data you want to capture.
- For sensitive data running on legacy systems, consider an on-premises solution that delivers management and monitoring capabilities within your firewall.
- Use standard security building blocks, which are inherently more secure due to industry review and upkeep, and are more reliable in terms of not having to change your systems later (when the non-standard blocks go away).
- Make designs more compartmentalized to better isolate and wall off cyberattacks.
- Use hardware-based root of trust security to provide essential security services and protect critical code, data, and hardware.
- The Digital Social Contract for IoT security is the foundation for long-term trust between technology providers and users.



Enabling businesses to securely create, deploy and manage IoT devices

Learn how Arm Mbed can simplify your IoT development at **mbed.com**

arm MBED

Step into the IoT future

The Internet of Things (IoT) is creating a global network of connected, intelligent devices that will inform and enhance society and business. Many important challenges and design considerations must be addressed early to build a complete and secure IoT solution. This book shows what is required to design a robust, scalable IoT solution serving a range of markets and needs, including important challenges to consider and why it is vital to address those challenges at the earliest stages of planning and design.

Inside...

- Explore IoT market opportunities
- Consider design choices
- Manage and update at scale
- Design for robust connectivity
- Protect code, data, and hardware

arm

Lawrence C. Miller has worked in information technology for more than 25 years. He has written more than 60 *For Dummies* books.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

Also available as an e-book

for dummies®
A Wiley Brand

ISBN: 978-1-119-50335-4
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.