THE THREE KEY ELEMENTS OF SUCCESS IN EDGE COMPUTING

EXECUTIVE SUMMARY

We live in an intelligent world. A host of devices shapes the way we live, from the cars we drive and the streets on which those cars are driven, to the power plants that generate electricity to the factories that make the goods we consume.

This intelligent world is the result of intelligent infrastructure. The Internet of Things (IoT) generates data that is consumed, transformed and used to drive automation through real-time analysis. This is the essence of edge computing. For the edge to live up to its promise, the integration of the edge-to-cloud-to-core datacenter must be seamless, secure and scalable.

Enterprises that extend cloud-native principles to the development and deployment of edge computing solutions help ensure a seamless and efficient edge-to-cloud journey. A services-based architecture can be distributed across the device, the edge and the cloud securely, with the mobility to deliver on resiliency and performance optimization.

Moor Insights & Strategy (MI&S) sees three fundamental elements to delivering the optimized edge-to-cloud environment: hardware and software standards that enable seamless integration, security embedded at the lowest levels of both hardware and software and a deep ecosystem that adheres to these standards and fully utilizes such security capabilities, enabling deployment at scale.

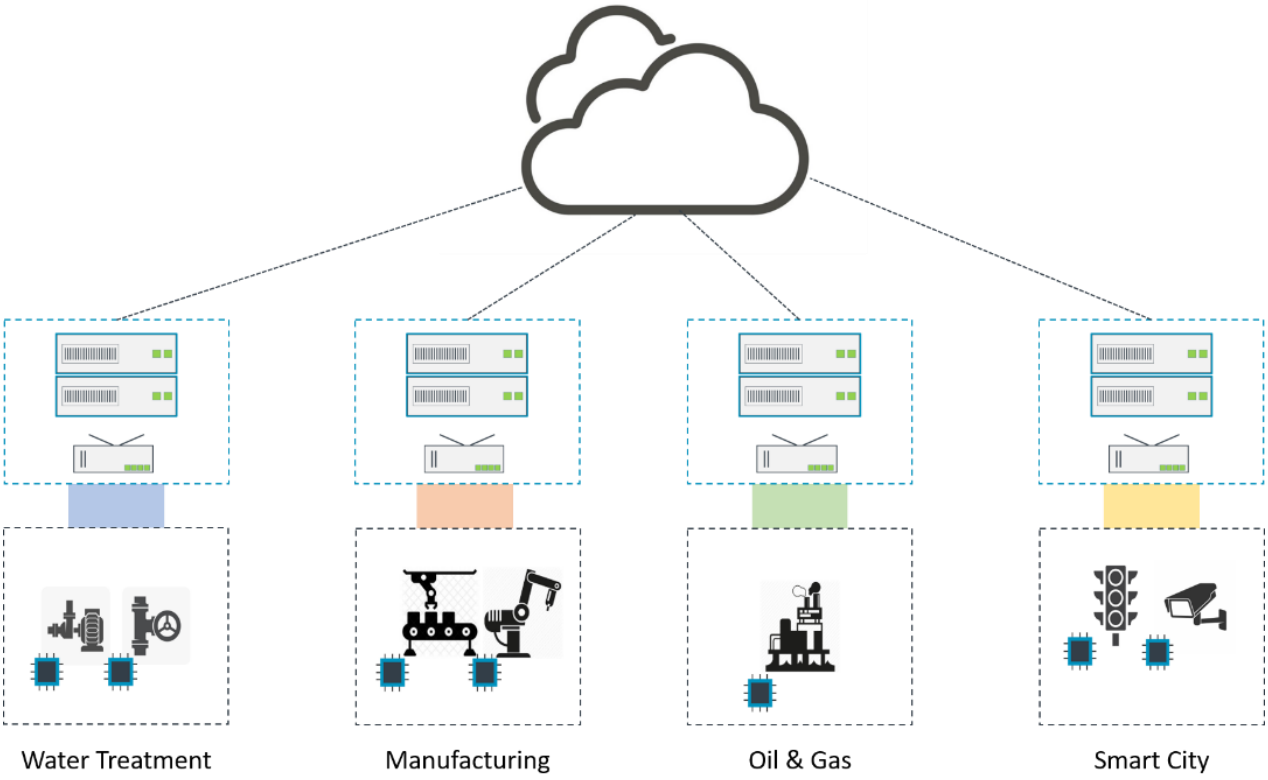
This paper will explore the challenges of edge computing and illuminate how Arm's Project Cassini overcomes those challenges by focusing on the three key elements of standards, security and ecosystem.

THE EDGE – SO DIVERSE, YET SO CONSISTENT

The edge can mean many things to many people. For this paper, we refer to the edge as computing environments outside traditional datacenter properties, whether that datacenter belongs to an organization or a cloud provider delivering services to an organization.

Even considering the scope mentioned above, edge computing is a market with many sub-segments, each with distinct needs – and a separate set of solutions providers. For instance, retail and manufacturing environments are different from each other and different from oil and gas or logistics environments. These industry differences include regulatory requirements, technology adoption rate, hardware and software requirements and support, and deployed security measures (both physical and cyber).

FIGURE 1: THE EDGE-TO-CLOUD JOURNEY



Source: Moor Insights & Strategy

We also include IoT, Artificial Intelligence of Things (AIoT), and Industrial Internet of Things (IIoT) devices in our definition of citizens on the edge for this research. It is important to note this, as it shows the many layers and vectors in this market.

- The equipment and devices that make up the operational technology (OT) environment will vary by industry. Each industry has a specific set of solutions providers that design and build the equipment and software that runs "the process."

    - The supervisory control and data acquisition (SCADA) platforms that manage the OT environment tend to be proprietary with industry- and environment-specific protocols for networking and management.
    - The edge environments deployed on-site are also specific to the industry in which they are deployed. Ruggedization, performance, power requirements and resiliency requirements drive industry-unique designs. Industry-specific ecosystems deliver the resulting products.
- While many IT solutions providers have edge offerings, the complexities of servicing every edge vertical make this task very difficult.

THE DATA JOURNEY

While these vertical markets may differ significantly in business operations, edge computing environments' essential purpose and functions are relatively consistent.

- ***Data capture.*** Be it a pump in a water treatment plant, a cash register in a store, a monitor in a hospital room or a meter in a power plant, machines and equipment all contain devices that are generating critical data that, in some cases, must be captured and acted upon in real time.
- ***Data Transformation.*** Computing resources on-site scrub data and transform it from raw values into a format that can be ingested and analyzed.
- ***Data Analysis.*** Using local gateways and edge servers, transformed data feed analytics tools look for anomalies and other conditions that will trigger actions. These actions tend to be an output that feeds the process control system driving the OT environment. For example, an out-of-bounds reading of water quality may cause a pumping station at a water treatment plant to shut down, with an alert sent to the plant operations staff.
- ***Data Backhaul.*** In addition to real-time analysis, a critical component of edge computing is understanding historical trends and deviations from those trends. Backhauling collected data to the cloud at a regular cadence and performing deeper levels of analysis against historical norms is what allows organizations to maximize investments in OT environments. Indeed, the smallest of corrections can lead to millions of dollars in direct and indirect savings.
- ***Data Archival.*** Finally, the collected data gets stored in multiple databases. In OT environments, raw data is held in a historian database that resides in the OT environment and a data warehousing environment that lives in the IT environment.

SECURITY EVERYWHERE OR SECURITY NOWHERE

Security in the data journey is only as strong as the weakest link. From physical to cyber and from the device to the cloud, security mechanisms must be in place for data at capture, data at work, and data in flight. Given the trillions of devices that will populate the edge, holistic security can seem impossible to achieve. It's not. Security requires an organizational approach that is equal parts people, process and technology. Further, an organization's security is only as strong as its weakest point, its greatest vulnerability.

Security that protects the entire organization ideally employs technology based on a common set of standards, enabling a seamless and secure chain of custody from the point of data origination to archival.

TECHNOLOGY IS CRITICAL, BUT THE CHALLENGE IS BIGGER

Technology matters. Intelligent, interoperable and performant infrastructure is the cornerstone of any successful edge-to-cloud deployment. That begins with silicon tailored for specific use cases and conditions and extends to the application, where distributed, cloud-native architectures deliver mobility and inherent resiliency.

As with infrastructure, software is key to enabling a successful edge deployment, from managing the OT environment to the tools that allow an organization to monetize the data generated at the edge.

The challenges facing edge deployments are not tied to infrastructure or software but ironically lie in the rush of innovation without a clear body of standards. This dynamic leads to gaps in interoperability and security along the edge-to-cloud path. Device manufacturers can create proprietary security protocols, for example, or applications and application frameworks can be developed without considering the range of deployment models and use cases in the market.

Further, though edge computing is relatively nascent, successful deployments must consider OT environments that have been in existence for decades, with equipment and devices that are equally old in some cases.

As edge computing progresses and the edge-to-cloud matures, success can only be assured by an industry that designs and develops solutions based on standards implemented in both hardware and software. Interoperability, portability, performance and security must be primary considerations.

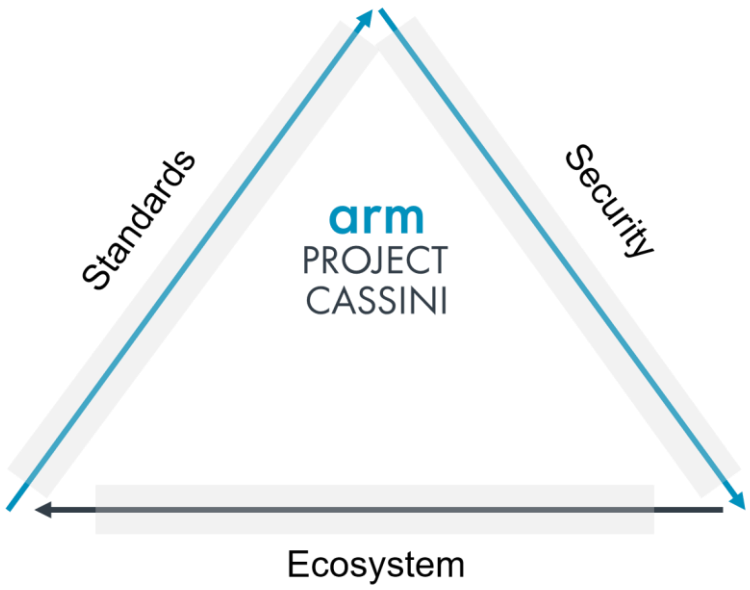
Given the diversity of the edge market and the variety of solutions, a logical question is whether it is even possible for the industry to coalesce around a common set of standards to drive edge adoption. MI&S believes it's not only possible, but it is happening through industrywide initiatives such as Arm's Project Cassini.

Arm is perhaps the best-positioned technology organization to deliver this set of standards and reference implementations. As an architectural IP provider, Arm enables systems designers to implement standards at the very lowest levels (silicon), which helps drive upstream adoption far more easily and more quickly.

Project Cassini is a set of solutions across a diverse edge and underpinning a diverse ecosystem that delivers on performance and security at the scale required from device to edge to cloud.

The result? An end-to-end edge solution that comprehends performance, security and scale from end devices through the edge infrastructure and the cloud.

FIGURE 2: THE PILLARS OF PROJECT CASSINI



Source: Moor Insights & Strategy

PROJECT CASSINI ADDRESSES THE EDGE IN ITS ENTIRETY

As mentioned previously, MI&S sees three fundamental elements to the delivery of edge solutions:

1. Hardware and software development rooted in standards, enabling seamless interoperability and multiple levels of performance optimizations.
2. Security that is built into the entire data journey, from the device to the edge to the cloud.
3. An ecosystem that develops cloud-native stacks and reference implementations that enable solutions providers to efficiently service the edge market with applications that can run anywhere, anytime and on any platform.

Again, these goals can seem deceptively simple, but they are extraordinarily challenging to achieve given the edge markets' diversity and the developed solutions. Arm introduced Project Cassini in 2019 to address these very needs.

STANDARDS

The power of the Arm hardware ecosystem is diversity. NXP, Marvell, Broadcom, Qualcomm and others develop a range of Arm-based CPUs for the edge and server market. Original design manufacturers (ODMs) and original equipment manufacturers (OEMs) build platforms on these CPUs – devices, gateways, networking gear and servers – that power the edge. These devices range in terms of power consumption, performance, durability and the like to support diverse environments and use cases.

One of the foundational pillars of Project Cassini is Arm SystemReady. This certification program assures all Arm-based systems adhere to a set of hardware and firmware standards, allowing developers to deploy cloud-native stacks with very little work. Simply put, standard Linux distributions and hypervisors "just work" on hardware designs that adhere to the Arm SystemReady standards, as these underpin most cloud-native stacks.

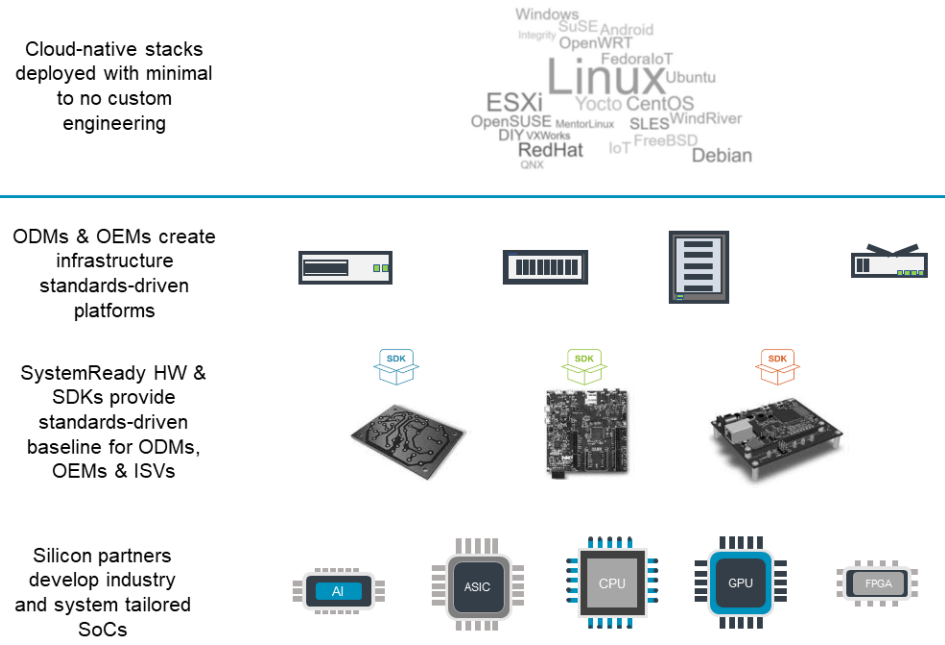
Perhaps most impressive about Arm SystemReady is the depth of the program, where multiple certification bands ensure a greater range of edge computing requirements is supported.

- *ServerReady (SR)* targets running standard and off-the-shelf operating systems and hypervisors within cloud and enterprise datacenters as well as server-grade systems at the infrastructure edge. This enablement simplifies the process of deployment and management of edge applications, as the OS and hypervisor are the root of the software stack.
- *Embedded Server (ES)* is about applying the principles of ServerReady to non-server hardware at the edge. For infrastructure and IoT edge deployments,

SystemReady-ES ensures that standard, enterprise-grade operating systems and hypervisors can seamlessly run on Arm platforms.

- *IoT Ready (IR)* is designed for programmable embedded platforms across varied market segments. SystemReady-IR ensures that commercial, custom or community distributions based on rich operating systems such as Linux can be run with minimal to no custom engineering effort. This should enable industry-specific solutions providers to more quickly stand up products, and allow consumers to more seamlessly deploy.
- *LinuxBoot Server (LS)* has been introduced to support hyperscalers using Linux-as-firmware (LinuxBoot). SystemReady-LS ensures that server platforms are suitable for deployment of the LinuxBoot firmware stack.

FIGURE 3 – FRICTIONLESS EDGE DEPLOYMENT WITH SYSTEMREADY



Source: Moor Insights & Strategy

The importance of SystemReady in enabling an open yet compatible ecosystem spanning the device to the cloud can't be overstated. The edge markets' diversity requires various tailored solutions that must be interoperable, secure and performant. These SystemReady bands enforce a set of architectural standards that enable precisely this. Further, the program's construct allows for Arm and its partners to add bands to meet these markets' needs as they evolve.

SECURITY

Security is perhaps the most significant barrier to organizations entirely investing in edge deployments. The devices and infrastructure that comprise the IoT-to-cloud edge employ a range of security mechanisms rooted in hardware and software, with little to no interoperability guarantee.

Arm has taken a unique approach with Project Cassini. The company positions its approach as creating a secure baseline for the edge.

- First, the company employs its Platform Security Architecture (PSA) Certified program, which Arm initiated with several partners in 2017. The program secures smart devices powering the home, connected space and IIoT market. As an element of Project Cassini, PSA Certified will be extended to support high-performance IoT and the edge infrastructure market.
- Second, the Arm SystemReady program includes a security profile that ensures hardware security features such as Arm TrustZone and Trusted Platform Module (TPM) are surfaced to software according to industry standards.
- Finally, Arm is a leading contributor to PARSEC. PARSEC (currently a project of the Cloud Native Compute Foundation), is security as a microservice. It enables connection of any cloud-native workload written in any language and packaged in any runtime container to any platform built on any architecture. It does this by leveraging various security mechanisms such as TPM, hardware security module (HSM), /trusted apps or custom security vaults. The PARSEC value proposition is:
    - The abstraction of resources through a common application programming interface (API), based on modern cryptographic principles, grounded in PSA
    - Security as a microservice, brokering access to hardware and providing isolated key stores for multi-tenant environments
    - A client library that exposes the API to developers in any programming language
    - An open-source project focused on enhancing the ecosystem

When looking at security on the edge, it is critically important to establish a security mechanism that spans the entire data journey, from devices and infrastructure to software and data. Arm appears to be delivering with Project Cassini.

ECOSYSTEM

The ultimate goal for any solutions provider in the edge space is to deliver products and solutions in the quickest amount of time, with the least amount of friction.

As seen in Figure 3, the ecosystem supporting the edge market is diverse and has many layers. To further demonstrate this ecosystem's complexities, consider that many edge "sub-segments" have their own ecosystems that can originate in silicon and often diverge at the ODM and OEM level. Each technology provider is looking to leverage the architecture and offerings of those that sit below them in the ecosystem, which can only be achieved through a common set of standards.

As part of Project Cassini, Arm enables its ecosystem through reference use cases the company calls reference implementations. These are best practices systems integrators and solutions providers can use in enabling edge deployments such as smart cities, oil and gas, universal customer premises equipment (uCPE) and the like. MI&S believes these reference implementations can prove invaluable to solutions providers and consumers, and the company should expand these across industrial markets.

One such example of Arm's success in driving cloud-native adoption at the edge can be seen in its partnership with open-source software company Rancher Labs. Rancher extended the capabilities of K3s, developing a lightweight container distribution designed to support any architecture, but optimized for Arm-powered edge platforms. This optimization drives use cases across different industries such as retail, energy, defense and aerospace. Customers have tens of thousands of sites with multiple edge devices at each location that needs to be managed efficiently at scale to extract value from IoT. Supporting these needs is possible with K3s deployed on a variety of Arm platforms that meet the desired cost, form-factor and specifications. The partnership's result is self-sustainability in edge and IoT deployments, enabling customers to focus on business outcomes. For more on this partnership, visit Rancher's blog.

MI&S PERSPECTIVE

ADDING IT ALL UP

Elements of the edge have been around for decades, from retail locations, industrial sites to remote and branch offices. As part of the digital transformation that many organizations are undergoing, monetizing the data generated in those environments is critical.

However, the lack of structure at the edge has kept organizations from fully embracing its potential. Interoperability from the device to the cloud, management at scale and security are all seemingly insurmountable challenges that have delayed IT and OT integration.

MI&S believes a common set of standards adhered to across the silicon, hardware and software development environments can lead to an acceleration of the edge computing market across all industries.

Further, Arm appears to be uniquely positioned in this era of the edge for several reasons:

- The Arm IP licensing model enables a diversity of solutions tailored for specific usage models, markets, devices and even customers. This model has resulted in:
    - A silicon ecosystem that aligns to its architecture, with industry- and device-specific vendors developing a range of compute engines on the Arm architecture
    - An architecture that spans the IoT-to-edge-to-cloud bridge, populating many of the devices that make up the IoT market today, much of the networking gear that drives the data journey and many cloud servers
    - A server ecosystem that spans high-performance computing to cloud computing to AI and advanced analytics
    - A cloud-native software ecosystem that complements and further enables the Arm hardware ecosystem, opening up the edge's true potential
    - The depth of the company's security IP portfolio enables perhaps the most comprehensive approach to locking down devices, infrastructure and data – at rest, at flight and at work.
    - The breadth of the company’s ecosystem in powering the edge, from devices to the cloud, is unrivaled.

The continued success of Project Cassini further enables the frictionless edge. A coalescing of standards around performance, interoperability, security and management brings a diverse hardware and software ecosystem together to meet the market's needs.

Although the ultimate success of Project Cassini is dependent on the ecosystem's adoption and utilization, MI&S sees Arm as being well-positioned.

For more information on Arm and Project Cassini, please visit www.arm.com/project-cassini.

IMPORTANT INFORMATION ABOUT THIS PAPER

AUTHOR
Matthew Kimball, Senior Analyst at Moor Insights & Strategy

PUBLISHER
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying the author's name, author's title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
This paper was commissioned by Arm. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.