W H I T E  P A P E R

# Standardization in Edge Device Firmware

## The Trusted Substrate Project

July 2021


**Abstract**

This white paper will look at the challenges faced by OEMs, open-source companies and industrial players in building and connecting secure IoT and embedded devices.

In particular this white paper will focus on the challenges of integrating a wide range of devices at scale while trying to ensure security remains intact. It will also look at the mismatch between hardware which often has a long lifetime versus embedded technology that has a much shorter lifespan.

While the use cases may differ one thing is clear - the need for standardization in firmware. Linaro and its member companies are driving this through the Trusted Substrate project.


**Contents**



**The Trusted Substrate project is a collaborative project for the integrated, tested and packaged foundation of open source secure boot and trusted execution elements. Linaro has a track record of bringing Arm vendors together on the Linux kernel and is currently extending this to firmware with Trusted Substrate.**

# Introduction - the Challenges of Deploying Edge Devices at Scale

Technologies such as IoT, AR, VR, Robotics and Machine Learning are increasingly part of our everyday lives. From wearable devices, virtual personal assistants and social media services to smart home hubs and video conferencing - chances are we all use some (if not all) of these use cases in some shape or form every day. The pandemic has made us even more dependent on these technologies as we work from home and keep in touch with loved ones virtually. During the pandemic, many homes have evolved into workspaces, which has sent demand for connected living solutions soaring.[1] By 2030, it is estimated that there will be more than 20 connected devices per human. We are moving towards a world where we are permanently online and always connected.[2]

While this connected world delivers countless benefits, it also presents challenges for those building the IoT solutions. How do you keep data secure and protect devices from cyber-attacks? How do you securely handle and process the constant stream of data on millions of connected devices in multiple locations? How do you keep devices up to date with the latest software? And how do you do all of this in a cost-effective and sustainable way?

Edge computing allows us to bring computation and data storage closer to the location where it is needed (the 'far' edge), saving bandwidth and improving response time.[3] But more is needed to secure and connect billions of such remote and diverse devices in a standardized way.

**The cloud provider's perspective:**

*"We live in a world where we continually distribute intelligent compute from clouds to the edge where the real value is at stake" says Eustace Asanghanwa. Principal Program Manager, Internet of Things Security R&D at Microsoft. "We live in a world where time to market is defined in months, not years anymore. We live in a world where users are demanding secure devices to achieve comfort in IoT."*

*"As a result, many solution providers who are building IoT solutions don't just take ownership of a device, they expect the OEMs to provide support of patches for 10, 15 years. This presents a challenge to OEMs - How do I support a device for 10-15 years when I'm consuming BSP components which are only supported for two years with infrequent patching? As a result, OEMs are reducing their SoC portfolios from 10 to 5 so they can manage the burden. This then becomes a challenge for IoT to proliferate."*

1. https://ww2.frost.com/news/press-releases/future-of-hyperconnectivity-offers-billion-dollar-opportunities-in-the-connected-living-ecosystem/
2. http://www.globenewswire.com/fr/news-release/2021/03/10/2190331/28124/en/The-Future-of-Connected-Living-The-Top-3-Connectivity-Ecosystems-that-will-Simplify-Human-Lives-Homes-Cities-and-Workplaces.html
3. https://www.cloudwards.net/what-is-edge-computing/

# Long Term Cost of Ownership

## An Industrial Manufacturer's perspective

Maintaining capital-intensive machinery is costly. It is made more costly by the mismatch between a long lifetime for the machine vs a short lifetime for the embedded 'smart' technology increasingly installed. OEMs are expected to support patches for the lifetime of the machinery, which in some cases is 10-15 years. Yet the board support packages they are consuming are only supported for two years and are often custom built. What is more, because the abstraction of bios/ firmware in Arm-based Industrial and IoT environments is not standardized, existing integrated solutions cannot be reused when porting to new platforms. This makes supporting these pieces of equipment extremely difficult, as without an abstraction of trust infrastructure, maintenance teams have to resort to per-platform customized fixes, validation and testing. This lack of standardization increases the total cost of ownership and makes long term support hugely labour intensive.

*"A permanent challenge is - how to bring updates - not just on the software side but also on the hardware side (on such machines) while keeping the software as stable as possible", says Christian Grabe, Project Director Digital Business at Bosch Rexroth." You can't afford to completely redesign your software architecture just because you upgrade the connectivity from e.g., 4G to 5G. From this point of view it is really important to have standardized interfaces which you can rely on and take from one device to another over the lifetime of the installation."*

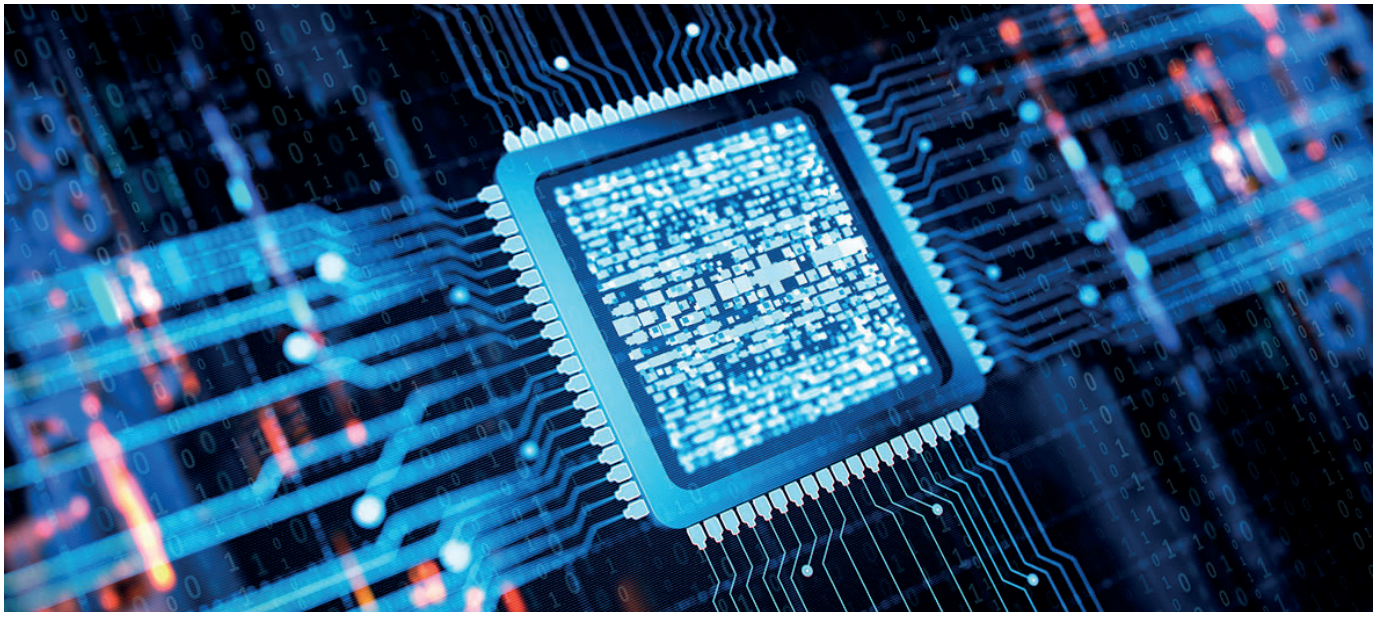
# The Burdens of Integration and Support

## A System-on-Chip Vendor's perspective

One legacy of the embedded origins of edge devices is that each SoC platform tends to have a specific boot sequence, creating the need for specific firmware versions to support a given SoC in order to be able to start the Linux kernel and applications. Firmware is often based on open-source elements and is usually from different projects. Although integrated into a product, they are independent for the purpose of updates and fixes and the source projects each continue to have their own life cycles. This means it is up to the SoC vendors to provide the right firmware versions and to make complicated integrations of all the software components, over a potentially very long lifetime.

The complexity of integration makes life difficult for SoC vendors for a number of reasons. It makes it harder to re-use software, increasing product development costs and time to market. The lack of standardization reduces their ability to be nimble and although vendor lock in may be seen as a short-term benefit for an incumbent supplier, a landscape of complex non-interoperable and unmaintainable bespoke solutions limits growth in the market for all players.

*"It is up to the SoC vendors to provide the correct versions and integrate all the complex software components", says Loïc Pallardy, STM32 MPU SW Lead Architect at STMicroelectronics. "That is part of the burden - complexity of integration. An efficient and effective validation of integrated firmware would allow us to standardize implementations and let design engineers select the development environment they want to use on our platform."*



# The Complexity of Secure Update Mechanisms

## An IoT Solution Provider's Perspective

There are multiple challenges which make securing and updating edge devices particularly difficult. More often than not, there is not just one single use case - there may be hundreds or even thousands. Implementing multiple custom software platforms for each different type of edge device, taking into account base SoC variations, design revisions and firmware versions, is not only costly but also requires considerable engineering resource. In order to support all these devices, companies need a single process which can handle a huge amount of diverse use cases.

To further add complexity, edge devices are much harder to secure because they are out of the data center and in the wild. Typically, edge devices will be spread out across multiple locations, which can be remote and difficult to access. Manually updating every single instance of a given edge device could end up a logistical nightmare. The ability to update devices remotely is not only practical but in some cases, such as security attacks, absolutely necessary.

*"Fundamentally it's time to think about scale from the start, both in terms of geography and device variation", says Peter Robinson, Principal IoT Architect at Red Hat. "If a customer has tens of thousands of devices out in the field under security attack, they want to be able to patch them reliably now rather than manually patching each individual device."*

# Working Towards a Standards-based Solution

**The challenges highlighted in this white paper demonstrate the burden on Industrial Manufacturers, IoT Solution Providers and SoC Vendors when building edge devices.**

*The Cost of Ownership*

The mismatch between the lifetime of a machine and the lifetime of the embedded technology, compounded by the lack of standardization, leaves industrial manufacturers no choice but to use up valuable engineering resource on per platform fixes.

*The Burden of Integration and Support*

The lack of integration between firmware components which often come from different projects with a range of life cycles - results in SoC vendors having to dedicate significant time and resource to making complicated integrations - often over an extended lifetime.

*Complexity of Secure Update Mechanisms*

The wide range of use cases and vast quantity of devices out in the wild make security particularly challenging. If IoT solution providers do not have the tools to centrally manage security fixes and software updates, they have no choice but to manually patch every single device. In the connected world we live in, this is not a viable solution.

In all the cases presented one thing is clear - the lack of standardization is costly for all parties involved. Everyone is spending an excessive amount of time on solving problems which are common to all. The only way to tackle these challenges is through open standards and open interfaces.

*Linaro has a track record of bringing Arm vendors together on the Linux kernel and is currently extending this to firmware with Trusted Substrate.*

# Introducing the Trusted Substrate Project

Trusted Substrate is a collaborative project for the integrated, tested and packaged foundation of open-source secure boot and trusted execution environments. The project brings standards based secure booting and over-the-air (OTA) updates to the most trust demanding embedded computing projects such as automotive and robotics.

*Firmware Standards*

Trusted Substrate is aligned with Arm standardisation and certification programs - specifically Platform Security Architecture (PSA) and System Ready.[4] It provides a path to reach and, more importantly, maintain compliance with these important initiatives which promote standards for firmware specification and trusted device procurement.

*Dependable Boot*

When exposed outside data centers, computers of all sizes are vulnerable to a whole new set of risks. Linaro's Trusted Substrate project aims to mitigate such threats as defined in various documents from NIST on firmware security or from the United Nations on Vehicle cybersecurity. One example of this is a key aspect of the Dependable Boot process in which BIOS behaves in a deterministic manner under physical attacks such as glitching.

*Over-the-Air Updates*

Other-the-Air (OTA) is a key value of Trusted Substrate as it allows firmware components to be updated with anti-bricking and anti-roll back protections. While OTA updates have been around for a while, they need to reach a degree of never-seen-before scalability and trust. Standard bricking and rollback protections of any updated BIOS component is a necessity. Whenever full transactional updates of complex boards with heterogeneous computing, accelerators and various microcontrollers take place, all firmware components need to be updated to a new version or not updated at all. And vouching for the successful update of a system (firmware, operating system, application software) should be flexible to accommodate rich policies.

*Trusted Services*

Trusted Substrate is being developed to facilitate portable Trust Services across processor architectures and platforms. For instance, Linaro expects to reduce the cost of developing and maintaining Trust Services such as Digital Rights Management and Digital Wallets.

*"Trusted Substrate provides good use cases and features which customers can use to develop their products on a given SoC", says Loïc Pallardy, STM32 MPU SW Lead Architect at STMicroelectronics. "These use cases have defined roles and responsibilities between all the different software components, certain APIs are clearly defined and this helps engineers integrate all the components while guaranteeing compliance between them. It is key that we can provide a complete integrated solution. Now with a unique API defined by EBBR with a UEFI interface, we have a clear contract between the firmware elements and the overall description of the system."*

**Trusted Substrate Functionality:**

- UEFI
- TPM 2.0
- U-boot
- OP-TEE
- TF-A
- Attestation
- Secure Boot
- OTA leveraging UEFI

**Infrastructure**

- Public repositories
- Inbound contribution management
- Continuous test and integration
- Release and lifecycle management
- LTS as an option

**Compliance**

- Arm Embedded Base Boot Requirements (EBBR)
- Arm Base Board Security Requirements (BBSR)
- Arm System Ready reference implementation

[4] More on this at https://www.arm.com/solutions/infrastructure/edge-computing/project-cassini

# How to find out more and participate

## Want to find out more about the project?

If you are keen to find out more about the project, you are welcome to visit the project page or join the working group call every second Thursday of the month, 2pm CET:

- Visit the project trustedsubstrate.org
- Join the Trusted Substrate Zoom call.

**Check if your board is supported by Trusted Substrate**

See the project wiki page at trustedsubstrate.org. At the moment we list supported hardware and in future we will also list supported firmware.

**Talk to us about how the Trusted Substrate project can help your business**

There are multiple ways to participate in the Trusted Substrate project and benefit from the standardization of firmware the project delivers. Membership is open to those interested in directly influencing the direction of the project to ensure it delivers the solutions they need. By becoming a member, your engineers get to work with Linaro's team of experts and other industry leaders on scoping and steering the solution.

For more information on membership, contact us on trusted-substrate@linaro.org.

---

### About Linaro

Linaro leads collaboration in the Arm ecosystem and helps companies work with the latest open-source technology. The company has over 250 engineers working on more than 70 open-source projects, developing and optimizing software and tools, ensuring smooth product roll outs, and reducing maintenance costs.

Work happens across a wide range of technologies including artificial intelligence, automotive, datacenter & cloud, edge & fog computing, high performance computing, IoT & embedded and mobile. Linaro is distribution neutral: it wants to provide the best software foundations to everyone by working upstream, and to reduce costly and unnecessary fragmentation. The effectiveness of the Linaro approach has been demonstrated by Linaro consistently being listed as one of the top ten company contributors, worldwide, to Linux kernels since 3.10. To ensure commercial quality software, Linaro's work includes comprehensive test and validation on member hardware platforms.

The full scope of Linaro engineering work is open to all online. To find out more, please visit: www.linaro.org and www.96Boards.org.