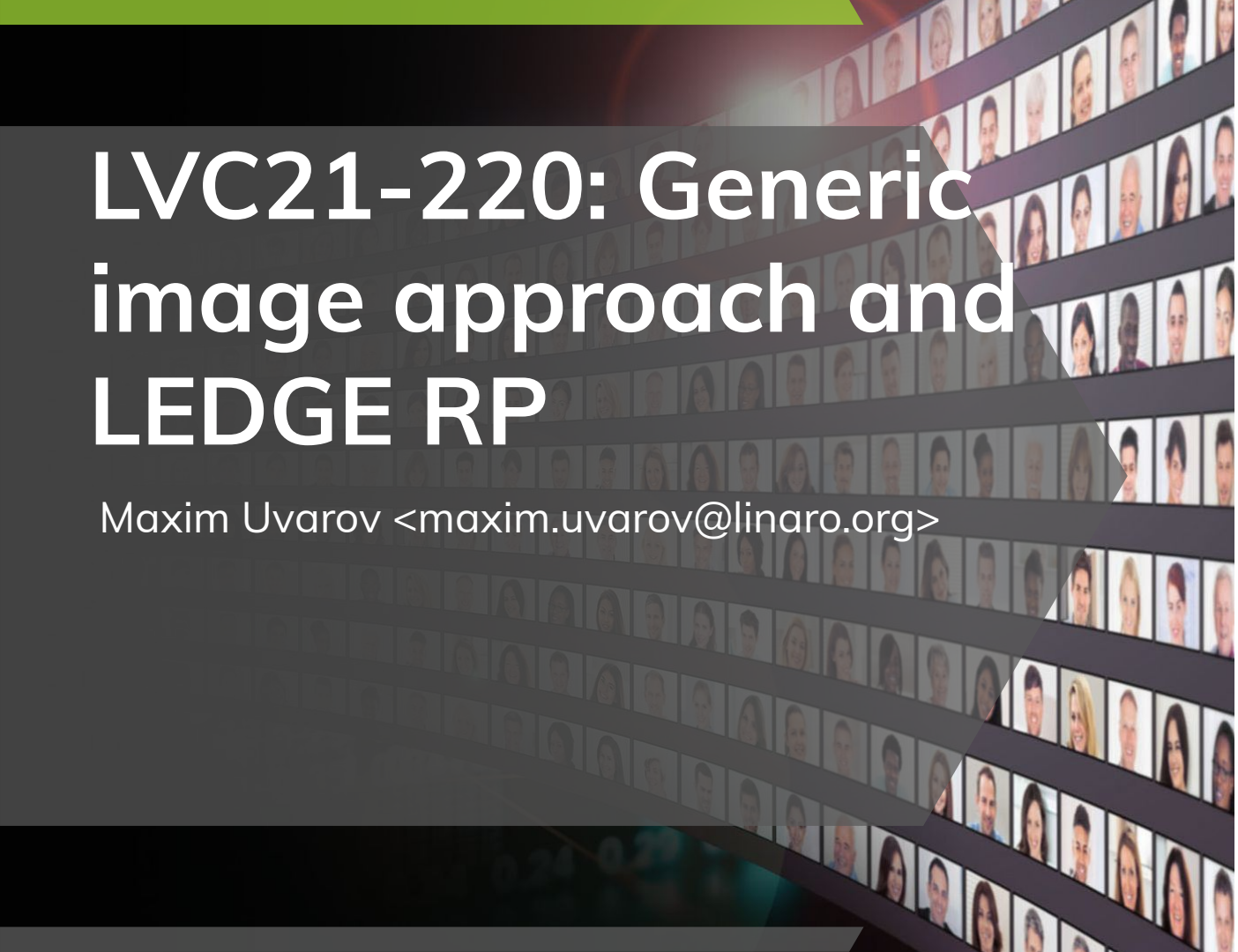
LVC21-220: Generic image approach and LEDGE RP

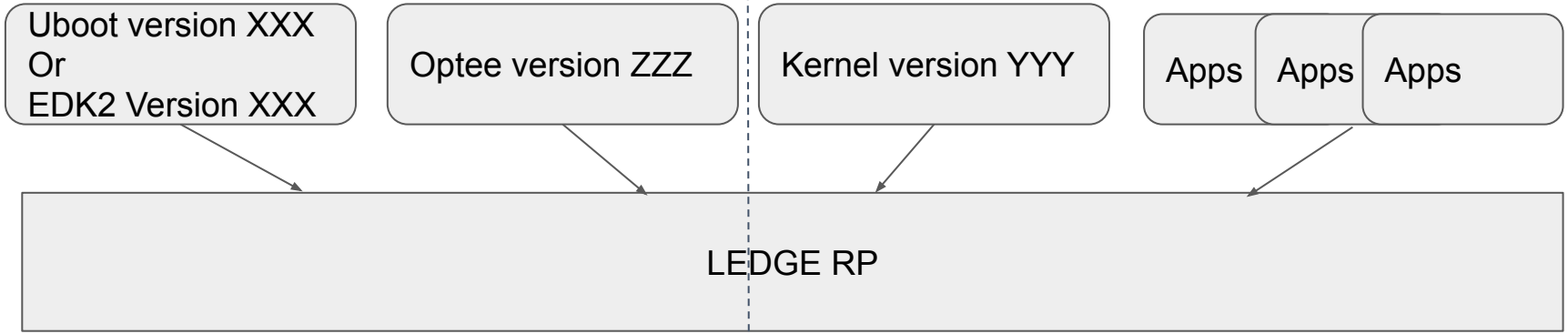
Maxim Uvarov <maxim.uvarov@linaro.org>



Linaro Connect
VIRTUAL • SPRING 2021

What is LEDGE RP?

Linaro's LEDGE RP is considered to be a reference platform for supporting industry standards for Linux operating system. Primary purpose is to build an operating system for IoT and EDGE devices observing specifications like UEFI, Secure Boot, EBBR, ACPI and etc.



TFA, OP-TEE, U-Boot - Trusted Substrate project

Linux kernel, userland - LEDGE RP project
(Independence of Firmware)

Why do we do LEDGE RP?

- Open Source development environment
- Single image for ARM, ARM64, x86-64.

Things we are working on are..

- Uboot loader UEFI support
- QEMU
- ARM Trusted Firmware-A
- OP-TEE
- Linux kernel
- Security (fTPM, Selinux, IMA, Parsec etc)

Platforms

- QEMU ARM (machine=virt,secure=on)
- QEMU ARM64 (machine=virt,secure=on)
- Stm32mp157c-dk2 (32bit ARM)
- Synquacer (64bit ARM)
- Ti-am572x (32bit ARM)
- QEMU x86_64

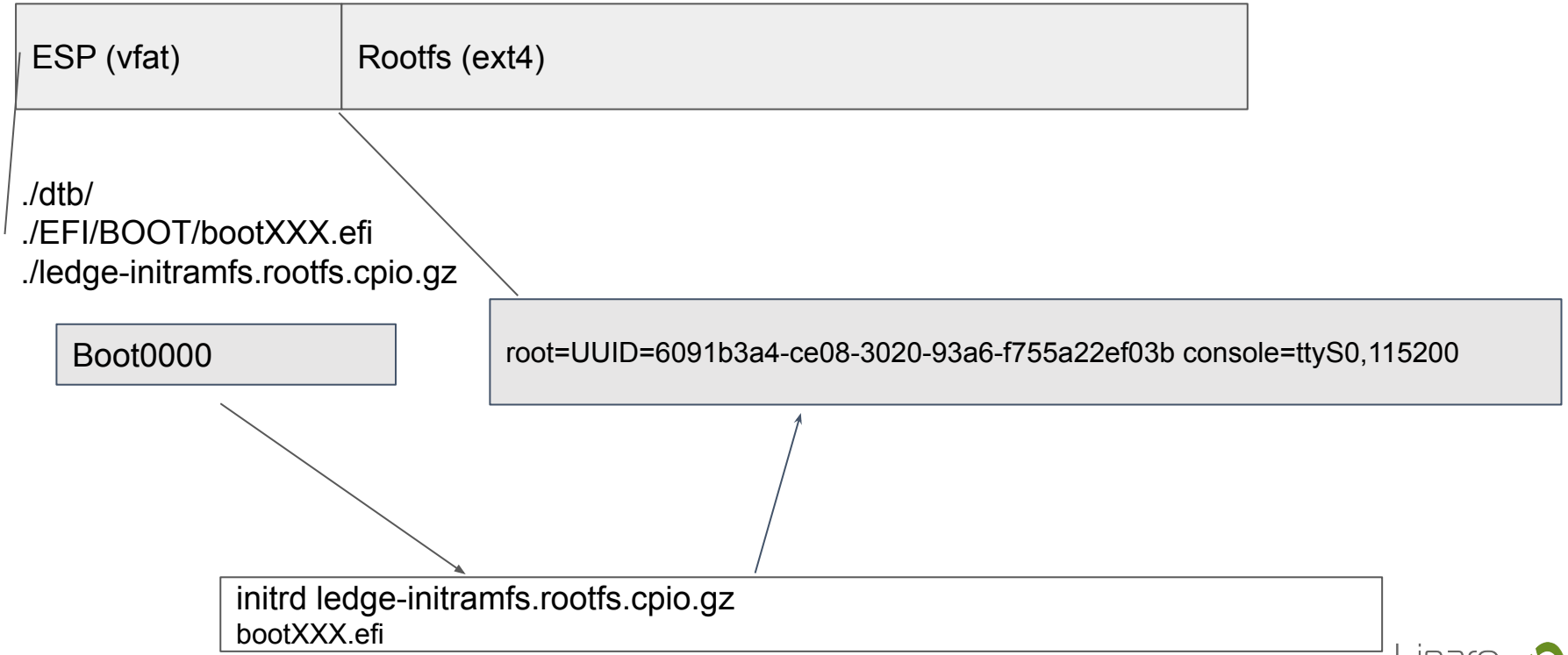
Internals: Images (wic, certs, bios)

Rootfs: ledge-gateway-lava-ledge-qemuarm64*.rootfs.wic.gz

Firmware: Firmware.uefi-edk2.bin/EFI_VARS.bin and firmware.uefi.uboot.bin/Sec_vars.bin

Certificates: ledge-kernel-uefi-certs.ext4.img

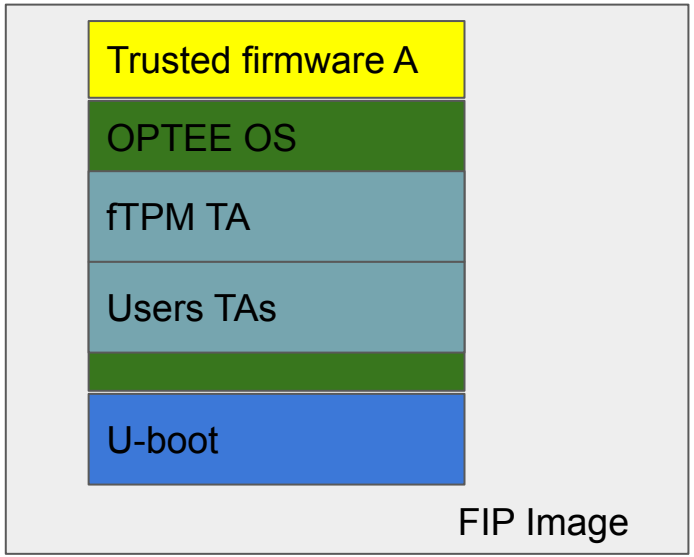
WIC image



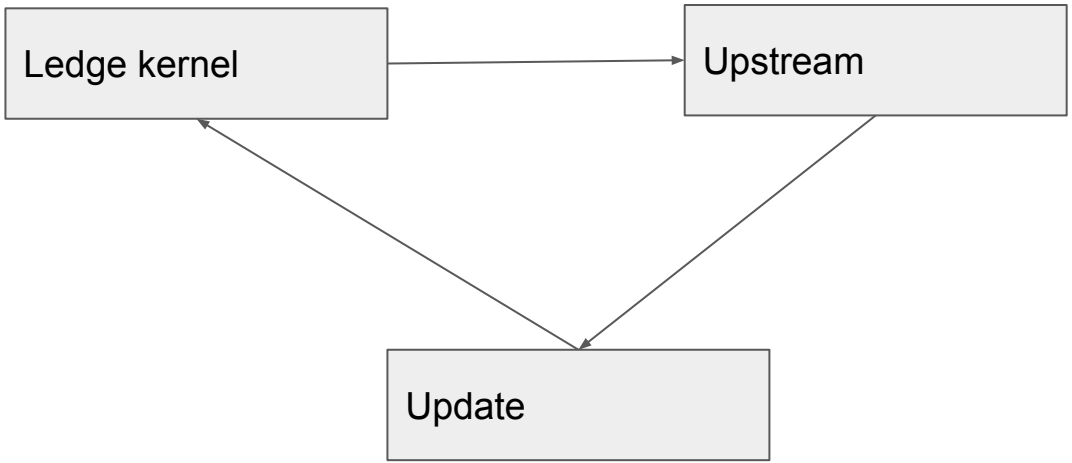
Firmware

- EDK2/Tianocore
- Trusted firmware A FIP image (BL1, BL32 (optee), BL33(ubot)

```
qemu-system-aarch64 -cpu cortex-a57 -machine virt,secure=on -pflash firmware.uefi.uboot.bin -pflash uefi_vars.bin
```



Kernel & Apps



Try to always upstream and use mainline versions of applications.

Images

Ledge-iot - the image for IoT devices. Package list and features are aligned to Fedora IoT

Ledge-gateway - image to support Edge gateways

We solved problems:

- fTPM as buit-in OP-TEE OS TAs
- U-Boot EFI Secure Boot
- U-Boot signed CapsuleUpdates
- Runtime variable support in U-Boot
- EFI variables in secure media (RPMB)
- QEMU reboot in secure mode
- Selinux labeling
- Parsec and Rust applications support on Open Embedded

Build, CI, Docs ...

Build and CI

https://ci.linaro.org/job/ledge-oe/

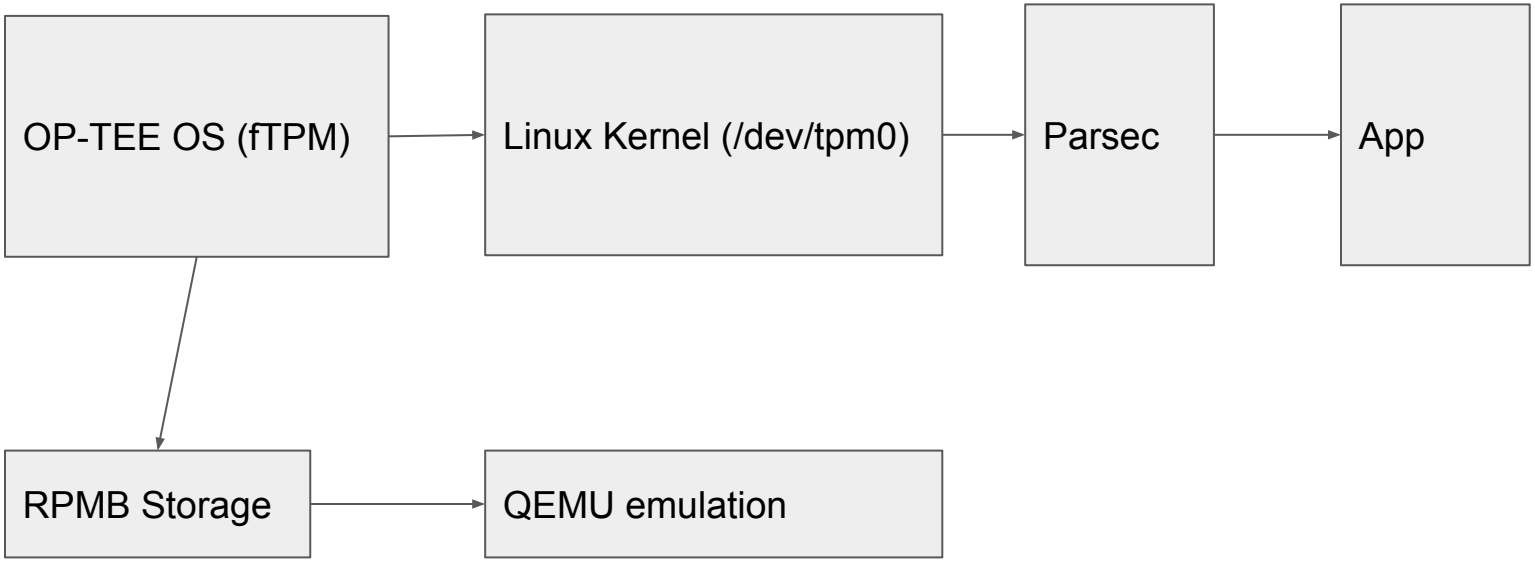
https://ci.linaro.org/job/ledge-oe-premerge-ci/

Docs
https://linaro.github.io/ledge-doc/

Binaries:
http://releases.linaro.org/components/ledge/
Dev: http://snapshots.linaro.org/components/ledge/oe/

Source code
https://github.com/Linaro/ledge-oe-manifest

Security

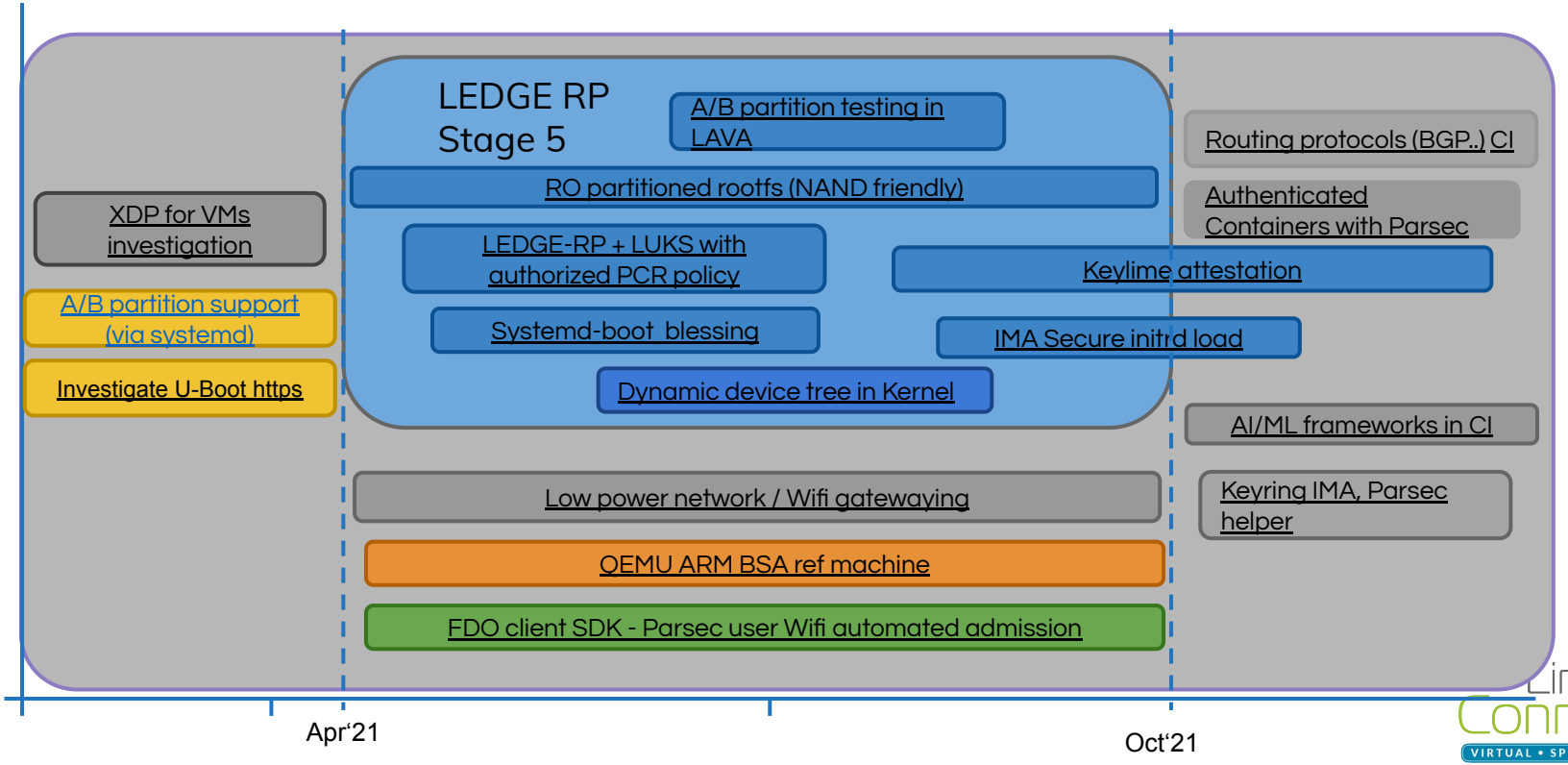

OP-TEE OS (fTPM)
Linux Kernel (/dev/tpm0)
Parsec
App
RPMB Storage
QEMU emulation

Projects linked to LEDGE RP

Trusted Substrate - support of Embedded Base Boot Requirements

- UEFI Secure Boot
- UEFI Measured Boot
- UEFI random number generation
- UEFI update capsules

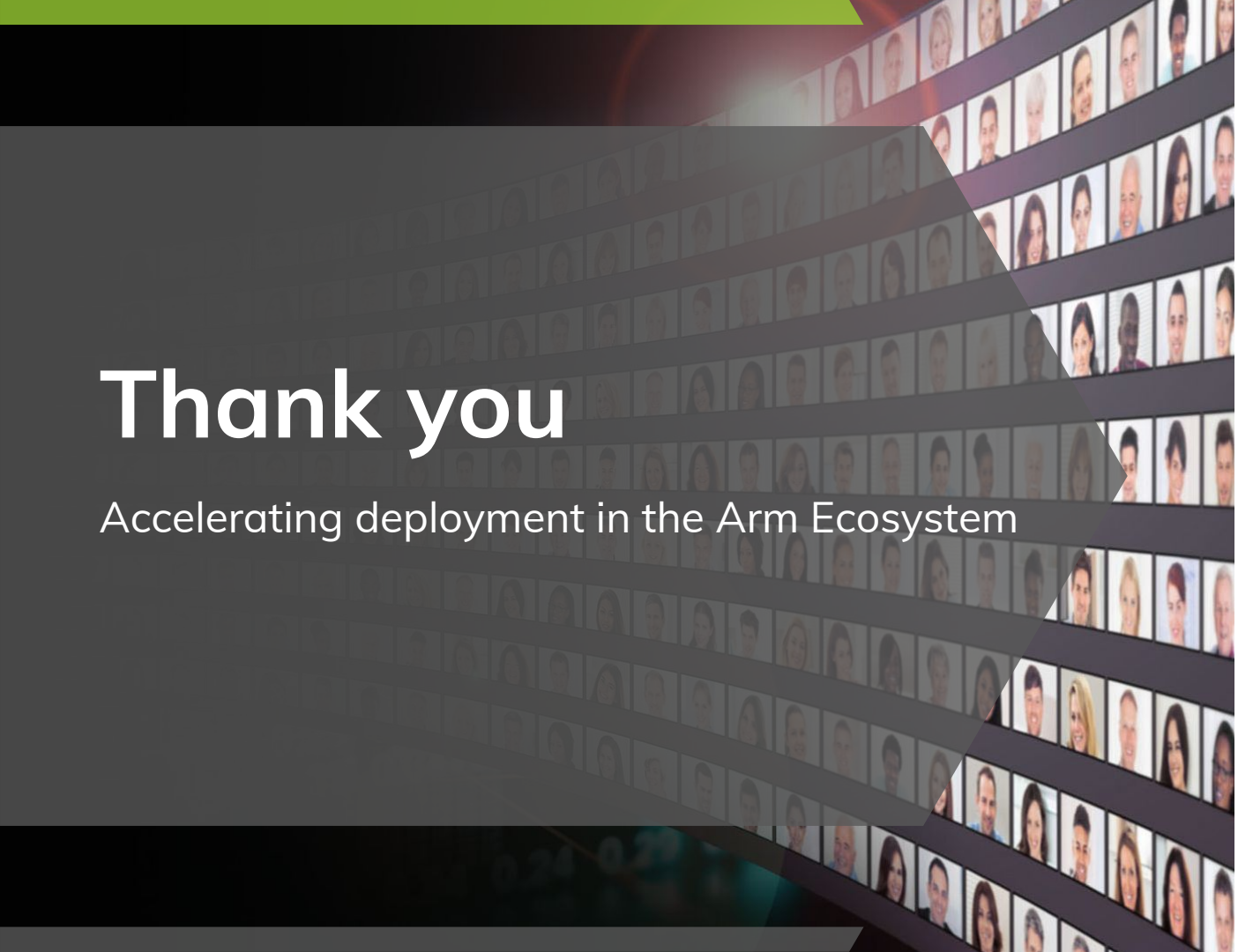
We are working on:



How to get involved?

https://www.linaro.org/engineering/edge-and-fog-computing/

Mailing list: team-ledge@linaro.org



Thank you

Accelerating deployment in the Arm Ecosystem

Linaro Connect
VIRTUAL • SPRING 2021