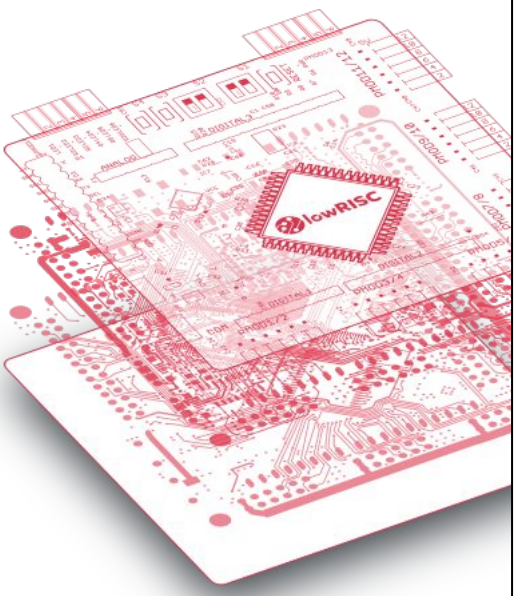
lowRISC

CHERIoT Enablement

Removing barriers to commercialization

Marno van der Maas



These slides and handout are part of a presentation for the TASER workshop as part of CHES 2023 given on 10 September 2023.

The full title of the talk is: Addressing the Challenges of the Commercial Adoption of CHERI with RISC-V in IoT and Embedded Use Cases

This presentation announces the CHERIoT hardware enablement project, which strives to get CHERI into the hands of engineers and remove barriers for CHERI adoption and commercialization.

If you have any suggestions for our base board, please have a look here: http://tinyurl.com/cheriot-fpga-board

CHERI is a technology that, instead of using standard memory pointers, uses capabilities that enforce bounds and permissions on each memory access. So why is CHERI important, what can it do?

To give you an idea of how powerful CHERI is; an analysis by Microsoft Security Response Center of all the vulnerabilities they reported in 2019 showed that at least 67% of them would be deterministically resolved if CHERI technology was widely deployed, see:
https://github.com/microsoft/MSRC-Security-Research/blob/master/papers/2020/Security%20analysis%20of%20CHERI%20ISA.pdf
This number could be much higher, since CHERI may be able to detect more of these vulnerabilities depending on the details of the implementation and failure modes.

Microsoft has already put significant effort into CHERI to make it useful for embedded systems. At lowRISC, we believe that RISC-V is the way forward and that embedded systems are a better place to start deploying CHERI than application class cores. This is because recompiling a whole rich operating system and all of the third-party applications that run on top of it with CHERI enabled is difficult, but in the embedded world there is more control over the software stack and doing a complete recompile might be quite reasonable.

We are also expecting security in IoT and operational technology to become much more important since cyber security liability is shifting onto manufacturers with the introduction of new laws.

Goals

Low-cost FPGA base system

Extended evaluation system

Open source RTL, board design and software

The goals of the CHERIoT hardware enablement project is to enable rapid development of CHERI.

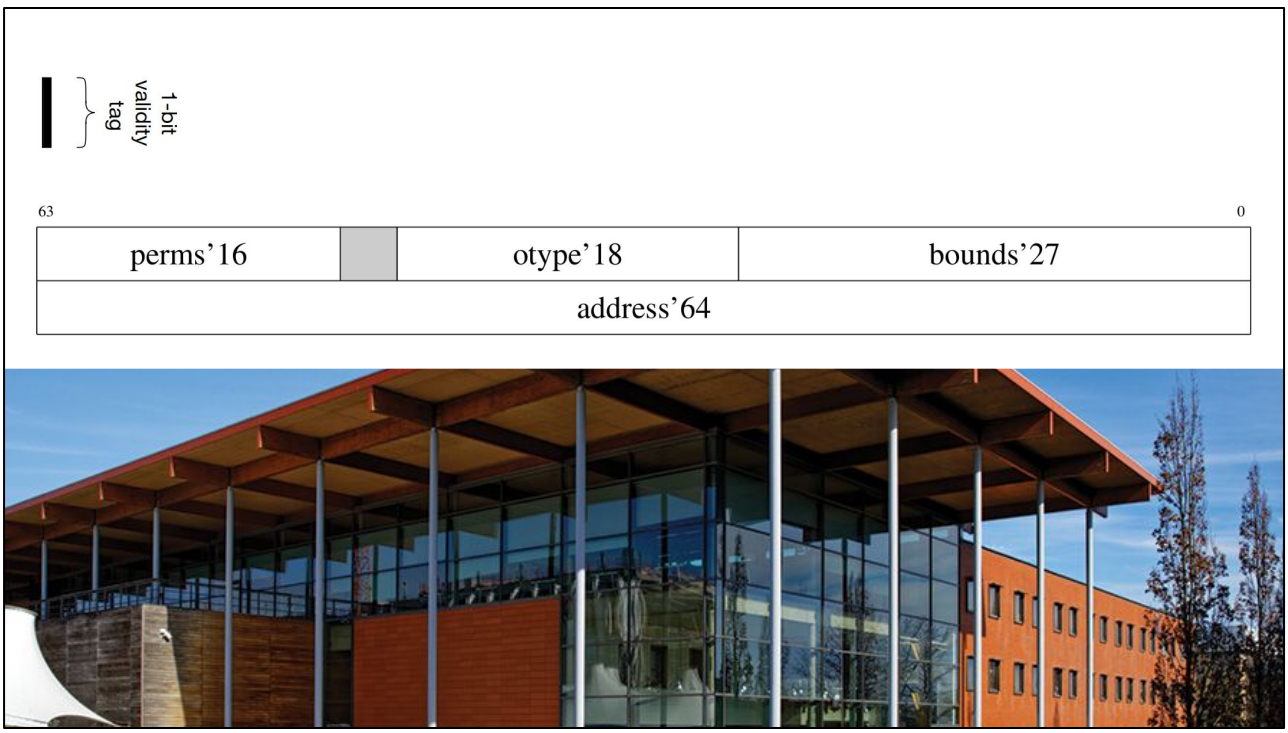
In the first instance, we will produce 100 low-cost FPGA boards that will be distributed in an outreach program to get them in the hands of the right people. They will also be commercially available beyond the initial 100.

In the second instance, we will create an extended evaluation version that requires a larger FPGA (so more expensive) but also using more mature IP. Both the base version and the extended evaluation version are important since they meet different needs.

All of our designs will be open source, including RTL, board designs and software. This is in line with lowRISC's mission to make open source silicon a reality.

Context

Let’s have a look at the background of CHERI, CHERIoT and lowRISC.

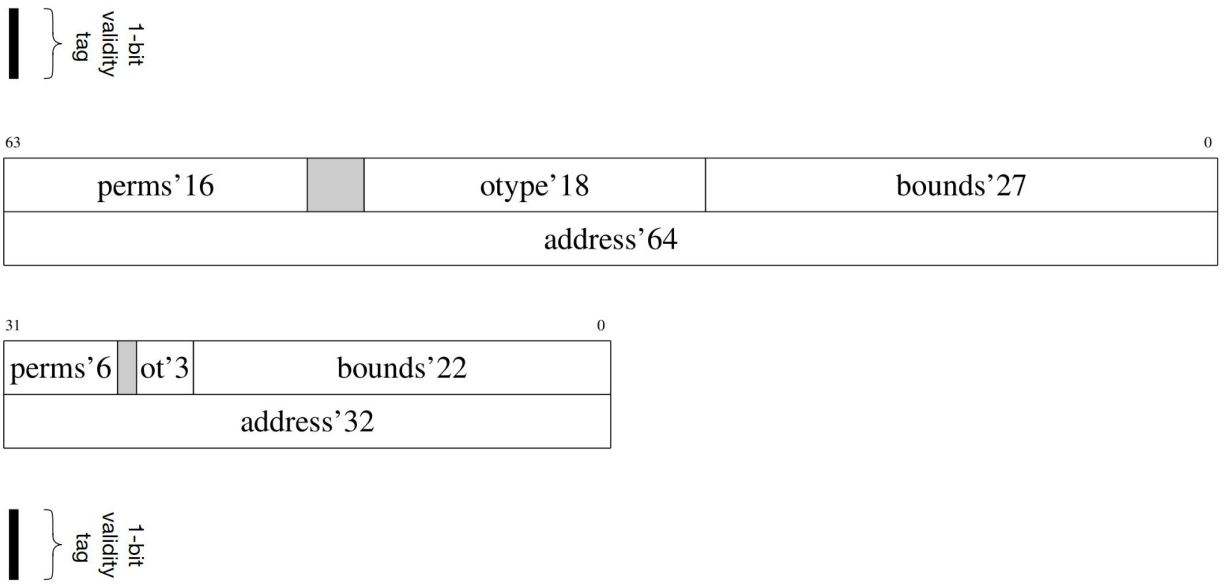


CHERI is a capability system that has been developed since 2010 at the Computer Laboratory at the University of Cambridge. Extensive research has gone into creating hardware prototypes, porting software, adding compiler support, etc.

On the top of the slide you see a 128-bit capability encoding a 64-bit address. This is the main capability format used in the current CHERI-RISC-V ISA.

CHERI capabilities include an address to a piece of memory, like traditional pointers do, but they also have associated metadata:

- Bounds: bounding the memory that is allowed to be accessed through this capability. For example, accesses can be kept within the size of an array.
- Permissions: fetch instructions, store/load data, store/load capabilities, etc.
- Object type: allows capabilities to be tagged as part of a compartment. For example, a library can pass a sealed pointer with a code entry point and a context to the user program and enforce that when the user program calls this capability it can only enter in one spot and with the correct context.
- Validity tag: this is stored out of bounds and is critical to the security of the capability system; any invalid operation to the capability will clear this bit.
  You might be wondering about the out of bound validity tag and its efficiency. This has been extensively tested in hardware and software to have as minimal impact as possible, see:
  https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201711-iccd2017-efficient-tags.pdf

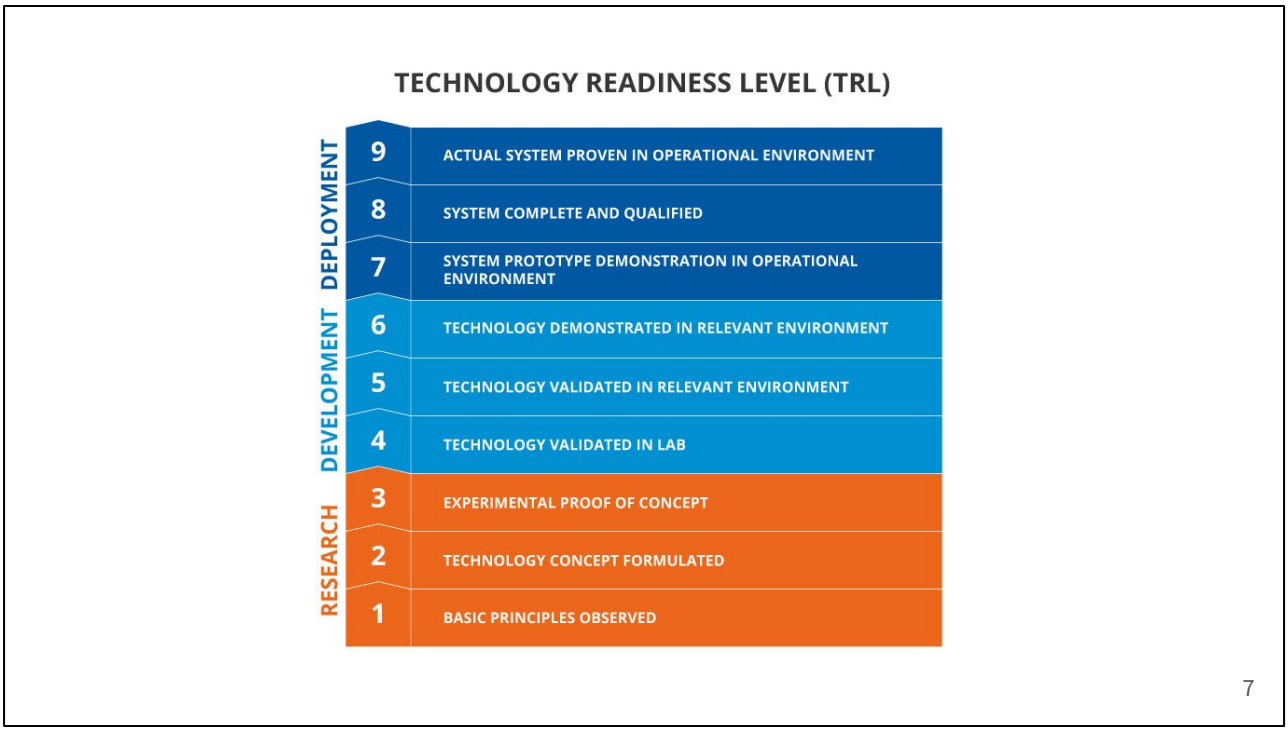


CHERIoT is an improvement to CHERI for embedded systems. You can see that it has a 32-bit address instead of the 64-bit address shown previously. It also only has 32-bits of metadata, which makes it difficult if you want to keep all the flexibility of the original CHERI. To make sure everything fits, they compressed the permission bits from 16 to 6 bits and made design decisions that limited the possible values of the otype.

The main CHERI project was focussed on backward compatibility and application-class processors. This was necessary to show that the technology could work in the most difficult of environments. However, when focussing on embedded systems, we don't have to worry much about backward compatibility, because we have much more control over the complete software stack. In CHERIoT, they removed hybrid mode and require all applications to run in pure capability mode, which also removes the need for a default data capability and a mode bit in the program counter capability:
https://www.microsoft.com/en-us/research/publication/cheriot-rethinking-security-for-low-cost-embedded-systems/

Microsoft has already done some great work with their newly proposed CHERIoT by taking lowRISC's Ibex core and making an initial version with CHERIoT support. It has also developed CHERIoT RTOS, which already works out of the box with pure capability support.
https://github.com/microsoft/CherIoT-ibex
https://github.com/microsoft/CherIoT-rtos

Because of the level of control of the software stack in embedded systems, we believe that embedded systems are the ideal platform to introduce CHERI in the wild because it is realistic to require all software to be recompiled.



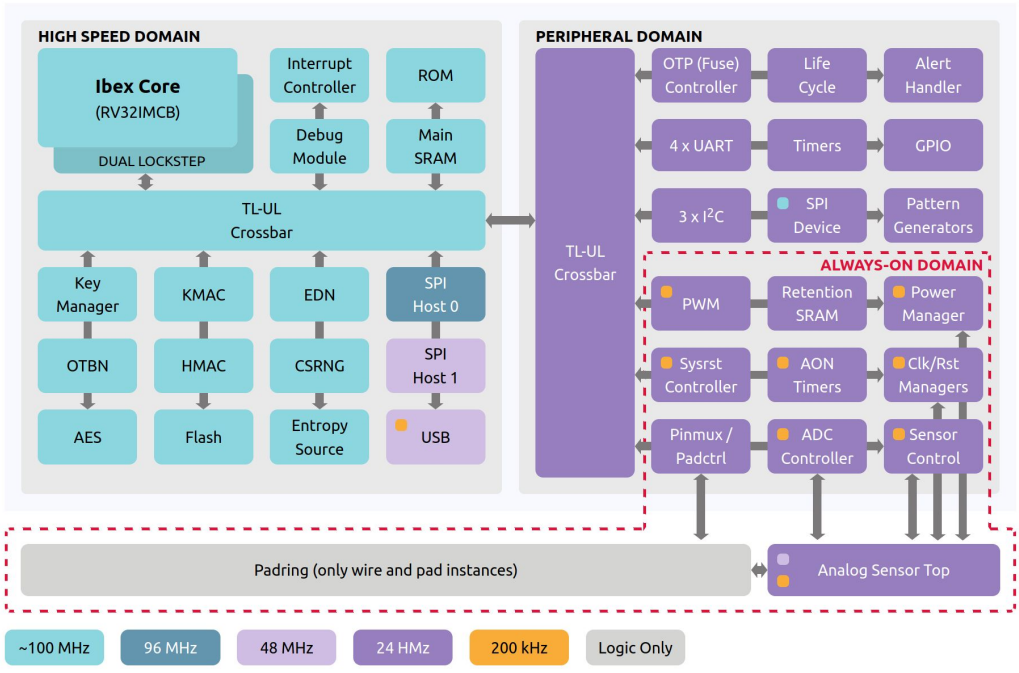
There is a lot of work that has gone into the research aspect of CHERI (steps 1-3 of TRL), and in recent years they have been pushing in the area of development (steps 4-6). We want to push CHERI and CHERIoT technology further up the development stages and into the deployment stages.

There has been some work in the development stages, for example Arm Morello has proposed an initial version of CHERI in the Arm ISA including shipping a number of demonstration boards. However, we believe a RISC-V platform based on open hardware/silicon will improve accessibility to this platform. This is especially true for embedded systems and thus a good way forward in the long run.

This project is driven by lowRISC and is supported by Microsoft and UKRI:

- lowRISC is uniquely positioned to enable the adoption of open silicon since that is our mission.
- Microsoft has already done a lot of work on CHERIoT, including Ibex and RTOS, to enable CHERI's adoption in the embedded space.
- UKRI has already funded many CHERI initiatives through the digital security by design project and will be coordinating the outreach program for the 100 low-cost FPGA boards.

We are excited to work together with these two main partners and with the wider CHERI ecosystem!



lowRISC has been working hard on the silicon commons, which is a library of open source, permissively licensed silicon IP. On the slide you can see a block diagram of the OpenTitan chip and all of the IP blocks that are within.

In the top left, you see Ibex, which is lowRISC's flagship core. It is a 32-bit RISC-V core started in ETH and now sets itself apart from other such cores by being production quality. It achieves this production quality by a rigorous verification setup and has been used in multiple tape-outs. It is also highly configurable and secure.

We want to bring our experience with the silicon commons and fully-verified, open-source silicon to the CHERI world!

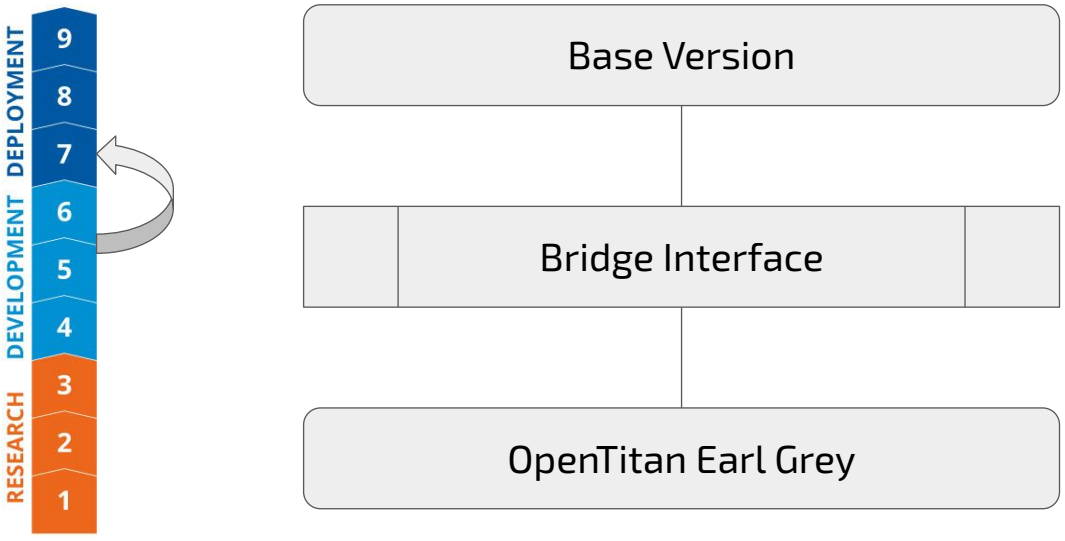
A little bit more about the OpenTitan project: This is an open source silicon root of trust. It is a multi-party, collaborative engineering project and we are so grateful to all our partners in this project, without them this would not be possible.

OpenTitan has given us experience in managing a massive collaborative open-source project. From its humble beginnings in the Computer Laboratory, CHERI has grown into a multi-party research project, similar to how OpenTitan is a multi-party engineering project.

It also means we have silicon security experience which lends well to the CHERI world.

Plan

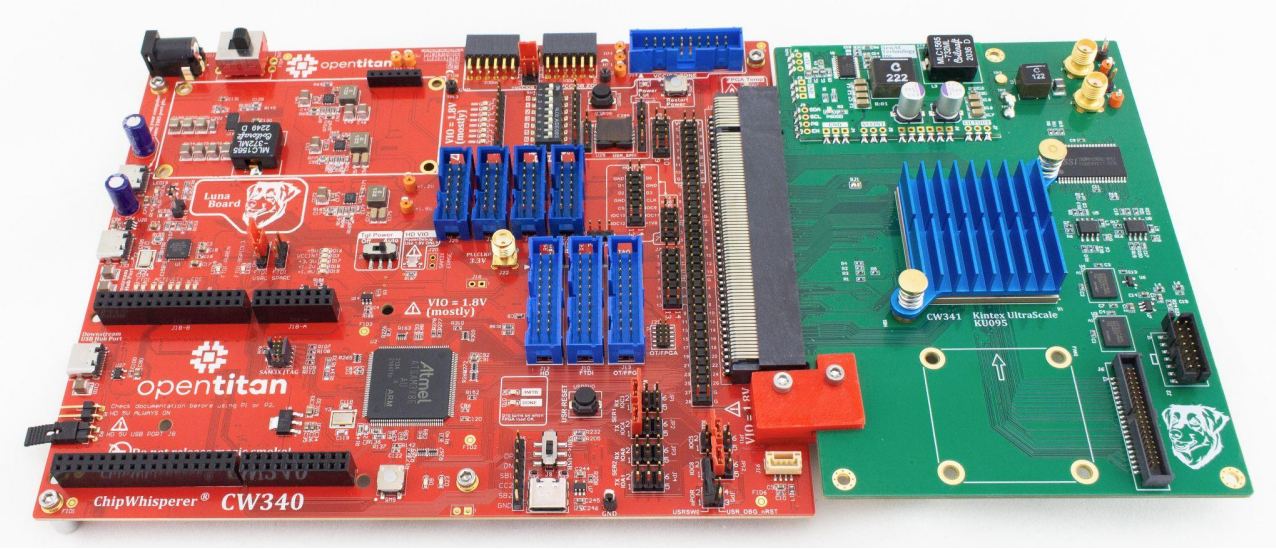
Now what's the plan with the CHERIoT hardware enablement project? What are we actually going to do?



12

The plan is really to boost the CHERI technology readiness level from the development stages into the deployment stages. Making sure that these boards get into the hands of engineers should help with that!

The block diagram on this slide shows how the base version will be extended with an OpenTitan chip and a bridge interface for the extended evaluation version. This enables Earl Grey to provide secure boot and other security services to a CHERIoT Ibex complex as well as giving CHERIoT direct access to certain peripherals (peripheral donation). It also builds on the security and maturity properties of the OpenTitan project, which has been taped out.



13

The picture on the slide is NewAE's CW340, this will be the more expensive board that can run the extended evaluation version. NewAE is part of the lowRISC family.

Before that, we will provide a low-cost FPGA board developed by NewAE. This will build on NewAE's experience making user-friendly hardware like the ChipWhisperer.

We will base our low-cost FPGA design on the Ibex demo system with its associate labs and then a bigger FPGA like the one shown in the picture for the enhanced evaluation version.

Low-Cost Board

FPGA:	Lattice ECP5 vs Artix 7
Headers:	PMOD, Arduino Shield, R-Pi Hat, mikroBUS Click
Interfaces:	USB, JTAG, SPI, LCD, ethernet, ADC
Any input?	**cheriot-bv-reqs@lowrisc.org**

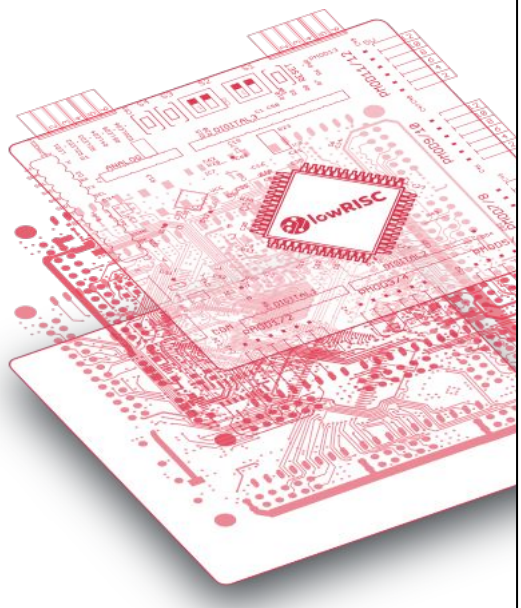
We are finalizing the design of the base board, on the slide you can see a few things that we are considering at the moment. We'll be finalizing the requirements by 25 September 2023. If you have strong opinions on anything you want on there then please send me an email. It is especially useful if you can tell which features you would prioritize over others.

We want to remove barriers to adopting the CHERI technology by providing this CHERIoT hardware enablement ecosystem. We believe in open source hardware and with making it high-quality so that it becomes the goto platform for a fully-verified and secure option. The CHERIoT hardware enablement project will be a first start at making this a reality.

Please feel free to provide feedback on board requirements through this form and/or email your suggestions.

lowRISC

mvdmaas@lowrisc.org



Thank you all for your attention, please let me know if you have any questions now or via email.

The QR code contains the handout of these slides plus accompanying text and links. If you can't open it send me an email, and I will send you a copy.

Please feel free to provide feedback on board requirements through this form and/or email your suggestions.