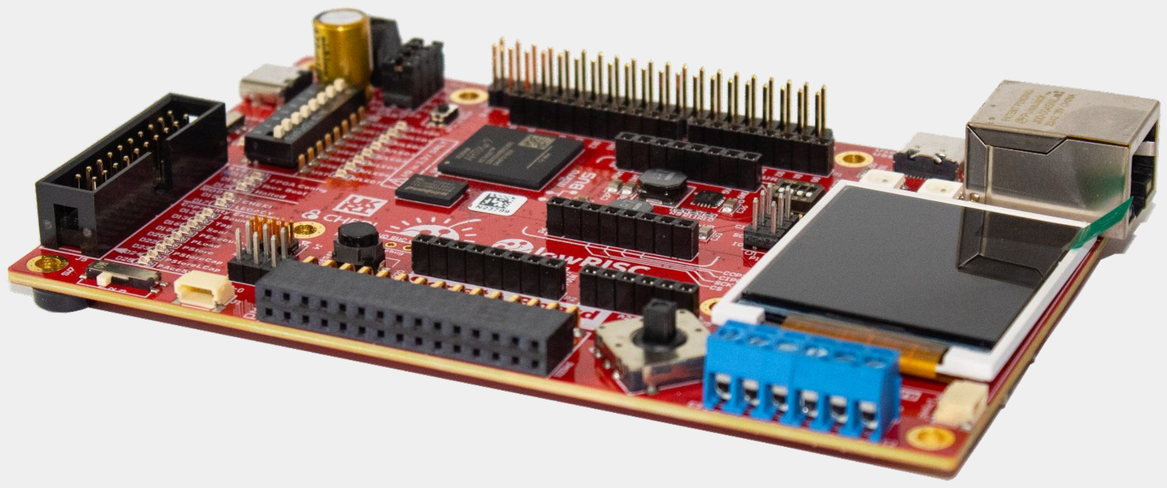
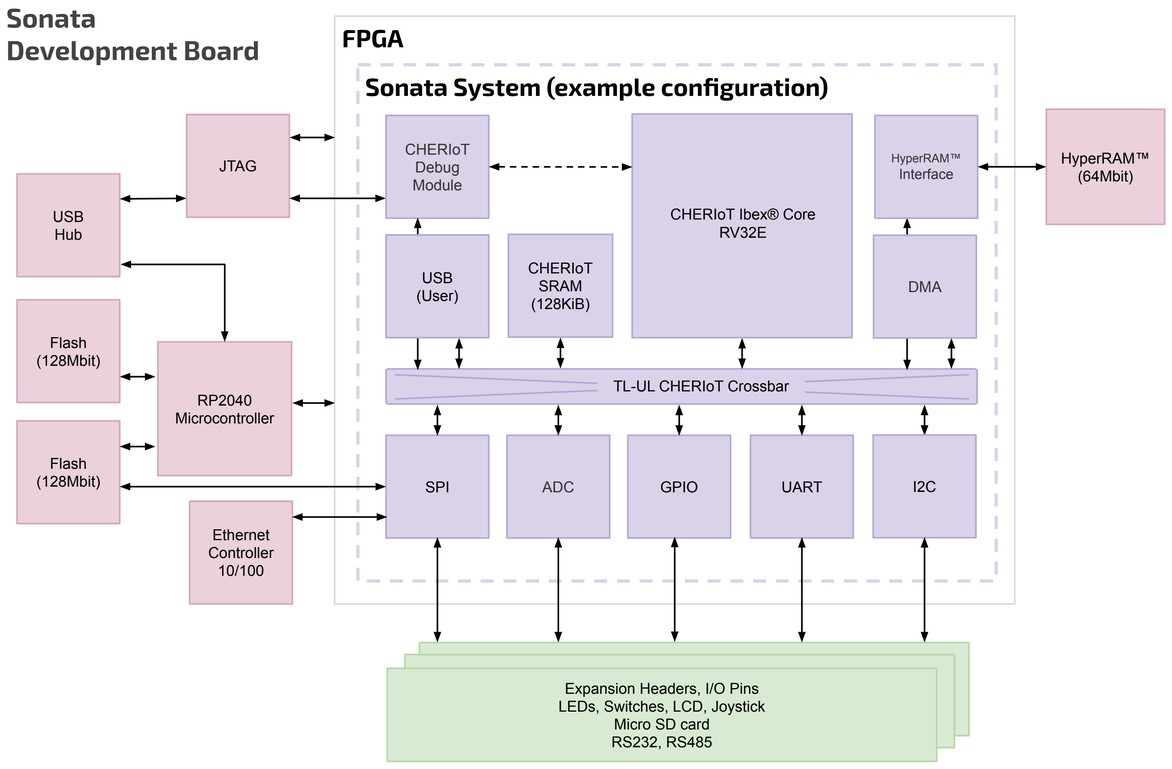
Sonata

Evaluating memory safety for embedded systems

The Sonata evaluation platform allows you to make your legacy embedded software memory safe in RISC-V by replacing pointers with hardware-enforced capabilities. The platform's PCB, RTL and software designs are all open source.

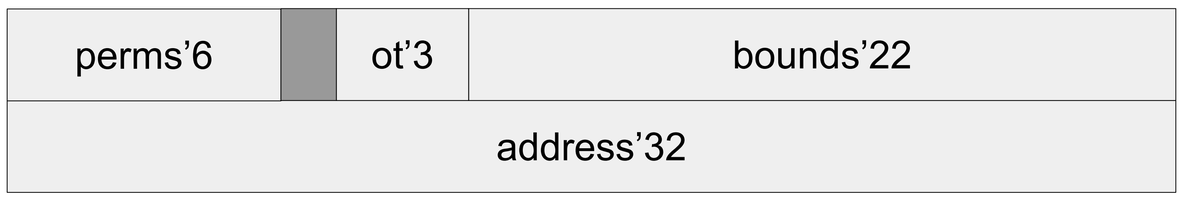




CHERIoT capabilities

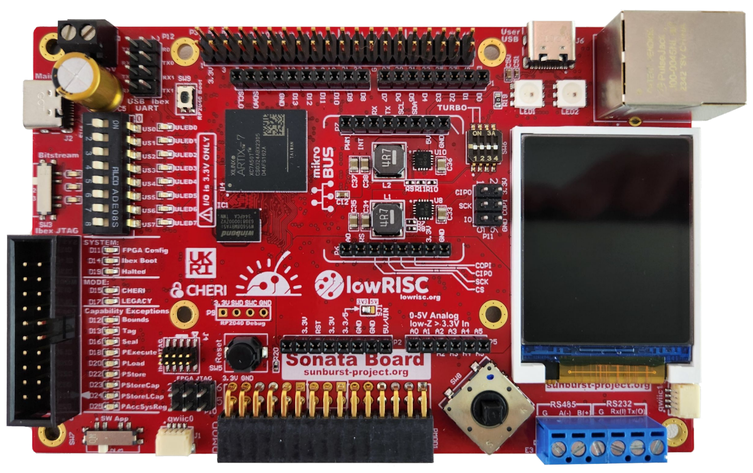
Developed by Microsoft for:

- Spatial memory safety
- Temporal memory safety
- Compartmentalization
- Specialized for embedded systems



Capability format:

- Validity tag bit (out of band)
- Compressed permissions
- Object type for compartments
- Bounds: base and top
- Memory address



sunburst-project.org

Site
Docs

lowrisc.org/sonata-system

Tag architecture

TileLink memory bus extended to support capability and revocation tags.

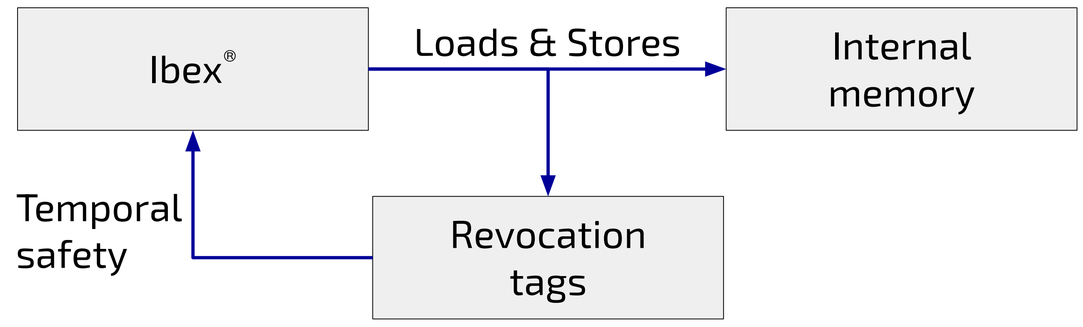
Host to device:

- valid
- opcode
- address
- data
- user
- ready

Device to host:

- valid
- opcode
- data
- user
- error
- ready

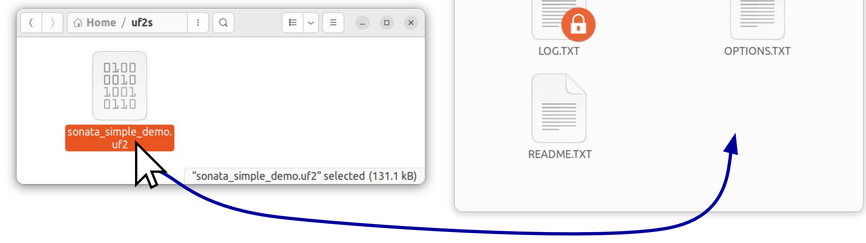
Capability tag



Revocation:

1. Set revocation tags for revoked memory
2. Sweep memory for revoked capabilities
3. While sweeping invalidate revoked capabilities that are loaded from memory
4. After sweeping clear revocation tags

Software development



- Drag and drop programming
- Board emulates a USB mass storage device
- Bootloader populates SRAM from flash
- Upstream CHERIoT RTOS support
- Compartmentalization examples and exercises

Delivered by Innovate UK, EPSRC and ESRC

DSbD

NewAE Technology

CHERI

lowRISC

Sonata, part of Sunburst, is funded by UKRI in support of the DSbD ecosystem (grant number 107540).