27/03/25

CHERI in SoC

Working Group Update

Ben Fletcher
Working Group Lead – CHERI Alliance

Agenda

- What is the working group’s mission?
- Current Activities and Status

What is the working groups mission ?

- The CHERI in SoC Working Group focuses on defining and standardising what needs to be included in a system to support CHERI.
  - We want to make it easier for people to build CHERI technology into their systems.
  - Explain the complexities and challenges of integrating CHERI technology into a system.

Current Activities and Status

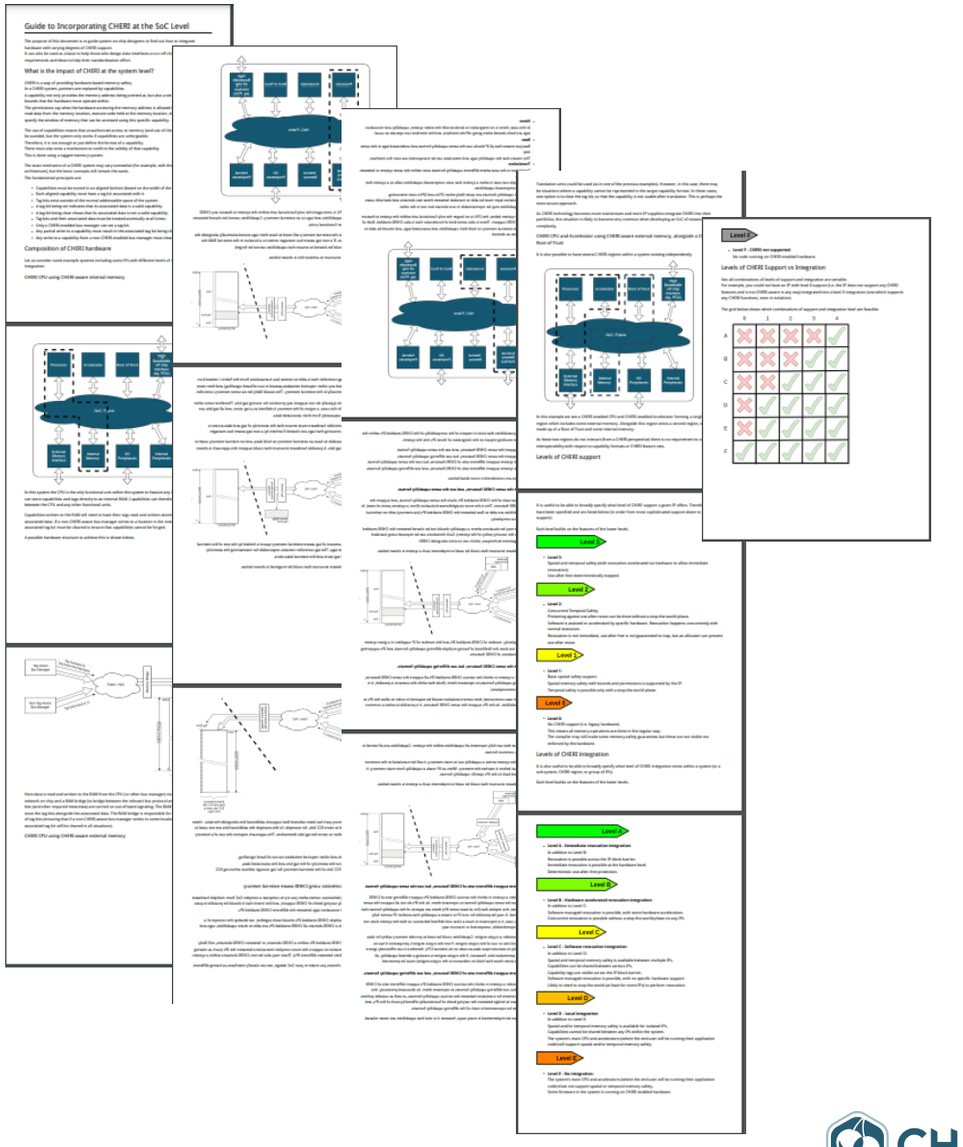
- We have written some material to help guide people into the world of building CHERI systems.
  - Our guide is a starting point, which assumes no prior CHERI knowledge.
- As part of the guide, we have proposed different levels of CHERI support, for both IP and systems:
    - To guide IP and system developers.
    - To aid comparison and selection of IP and systems.

Guide to Incorporating CHERI at the SoC Level

- Developed by working group.
- Received both internal and external review to the working group.
- Already used with 2 external IP companies to assist with CHERI ramp-up.

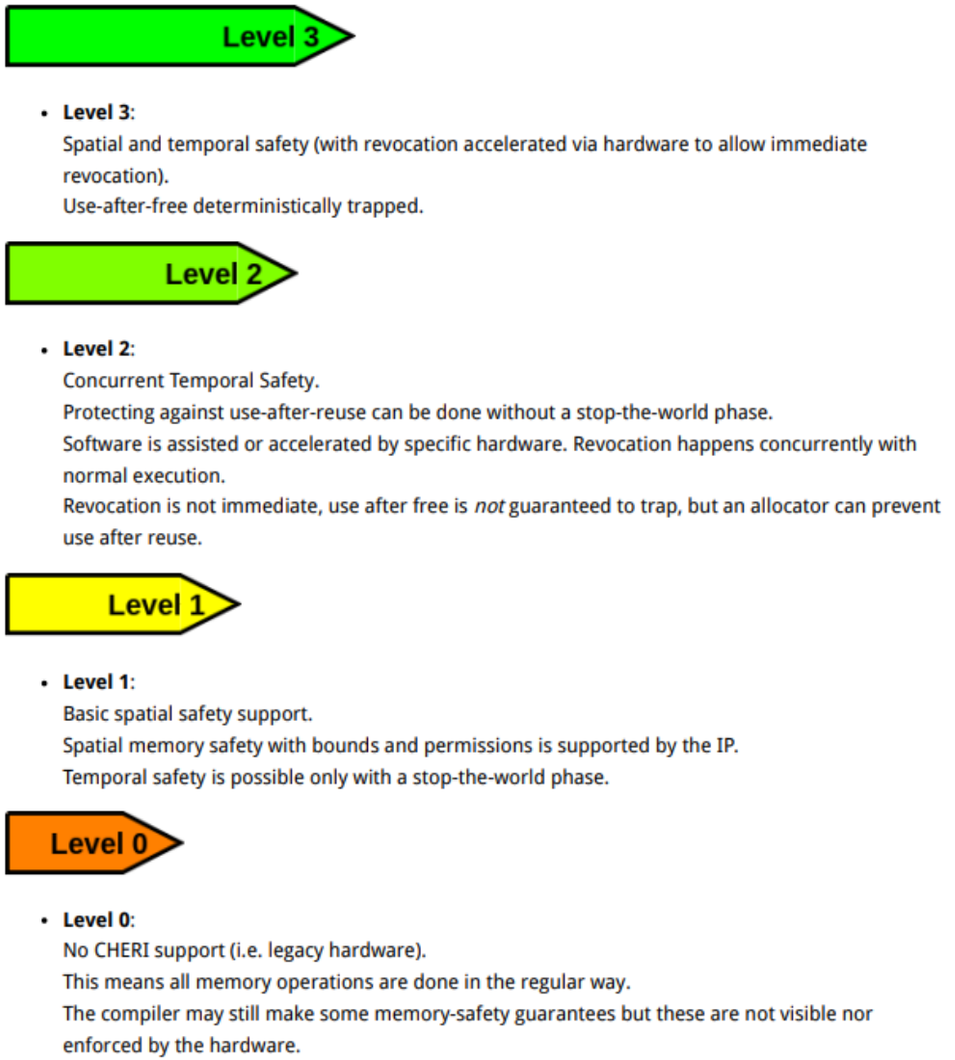
  Available on github:

  - https://github.com/CHERI-Alliance/SoC-System-WG/blob/main/guidance.md



4 levels of IP Support

- Level 0:
  - No CHERI support
  - Note that the compiler may still be able to make some memory-safety guarantees.



- **Level 3**:
  Spatial and temporal safety (with revocation accelerated via hardware to allow immediate revocation).
  Use-after-free deterministically trapped.

- **Level 2**:
  Concurrent Temporal Safety.
  Protecting against use-after-reuse can be done without a stop-the-world phase.
  Software is assisted or accelerated by specific hardware. Revocation happens concurrently with normal execution.
  Revocation is not immediate, use after free is *not* guaranteed to trap, but an allocator can prevent use after reuse.

- **Level 1**:
  Basic spatial safety support.
  Spatial memory safety with bounds and permissions is supported by the IP.
  Temporal safety is possible only with a stop-the-world phase.

- **Level 0**:
  No CHERI support (i.e. legacy hardware).
  This means all memory operations are done in the regular way.
  The compiler may still make some memory-safety guarantees but these are not visible nor enforced by the hardware.

CHERI

4 levels of IP Support

- Level 1:
  - Basic spatial memory safety.
  - Temporal safety is only possible with a stop-the-world phase.

- **Level 3**:
  Spatial and temporal safety (with revocation accelerated via hardware to allow immediate revocation).
  Use-after-free deterministically trapped.

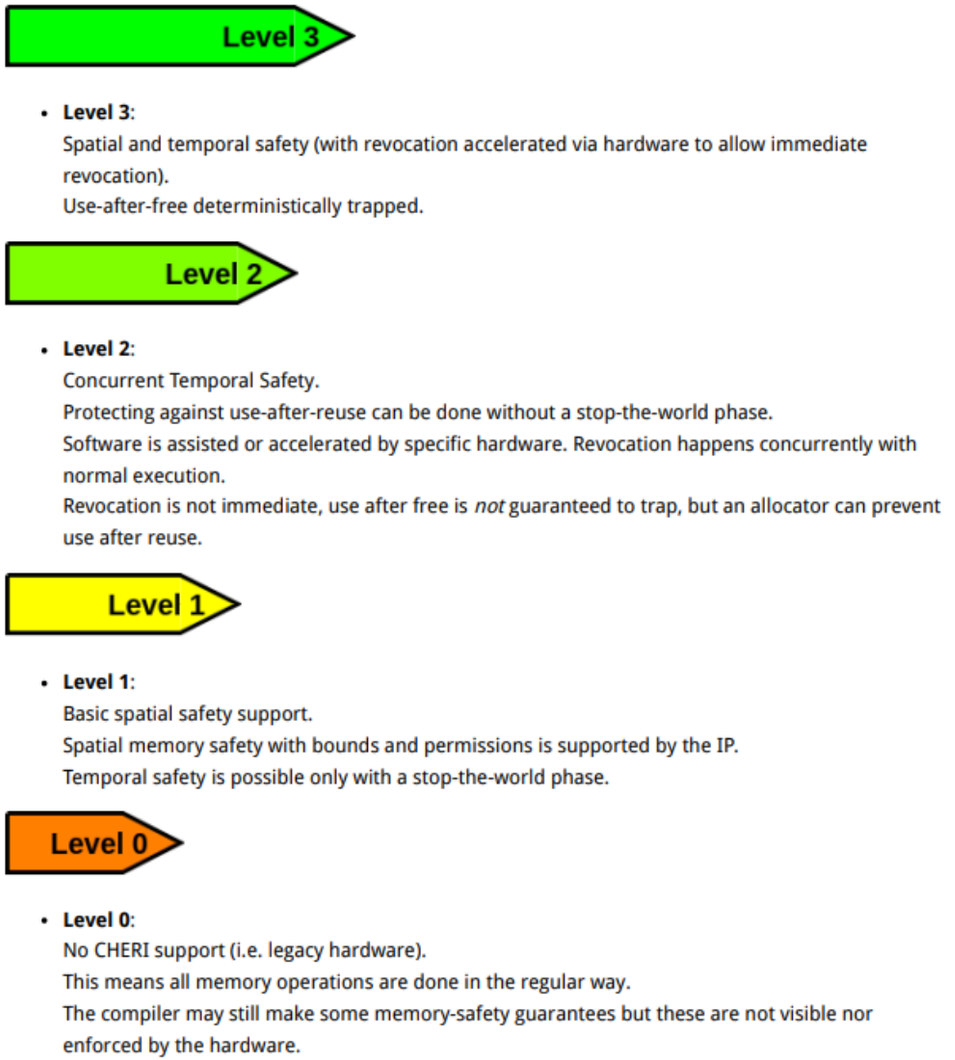
- **Level 2**:
  Concurrent Temporal Safety.
  Protecting against use-after-reuse can be done without a stop-the-world phase.
  Software is assisted or accelerated by specific hardware. Revocation happens concurrently with normal execution.
  Revocation is not immediate, use after free is *not* guaranteed to trap, but an allocator can prevent use after reuse.

- **Level 1**:
  Basic spatial safety support.
  Spatial memory safety with bounds and permissions is supported by the IP.
  Temporal safety is possible only with a stop-the-world phase.

- **Level 0**:
  No CHERI support (i.e. legacy hardware).
  This means all memory operations are done in the regular way.
  The compiler may still make some memory-safety guarantees but these are not visible nor enforced by the hardware.

4 levels of IP Support

- Level 2:
  - Concurrent temporal safety.
  - Revocation happens concurrently with normal execution but is ***not*** immediate.
  - Use-after-free is not guaranteed.
  - An allocator can prevent use-after-reuse.



- **Level 3**:
  Spatial and temporal safety (with revocation accelerated via hardware to allow immediate revocation).
  Use-after-free deterministically trapped.

- **Level 2**:
  Concurrent Temporal Safety.
  Protecting against use-after-reuse can be done without a stop-the-world phase.
  Software is assisted or accelerated by specific hardware. Revocation happens concurrently with normal execution.
  Revocation is not immediate, use after free is *not* guaranteed to trap, but an allocator can prevent use after reuse.

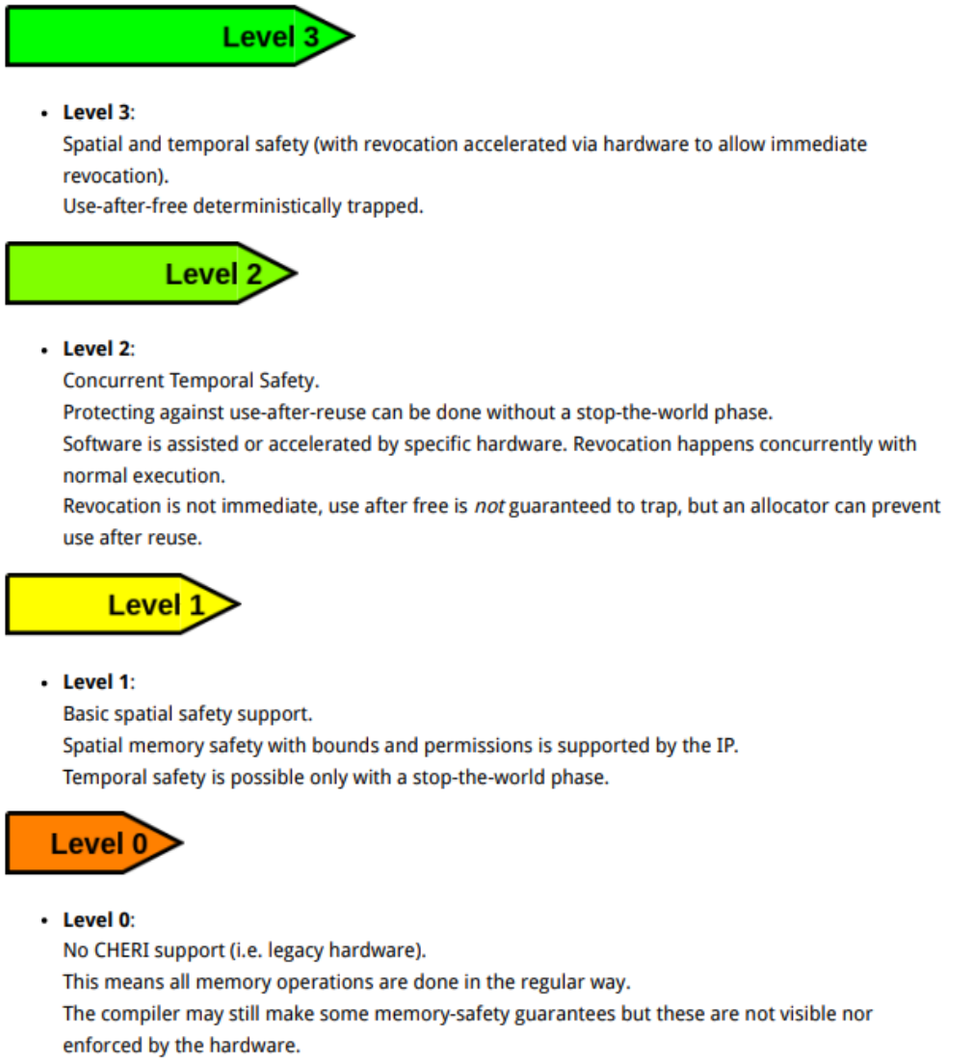
- **Level 1**:
  Basic spatial safety support.
  Spatial memory safety with bounds and permissions is supported by the IP.
  Temporal safety is possible only with a stop-the-world phase.

- **Level 0**:
  No CHERI support (i.e. legacy hardware).
  This means all memory operations are done in the regular way.
  The compiler may still make some memory-safety guarantees but these are not visible nor enforced by the hardware.

CHERI

4 levels of IP Support

- Level 3:
  - Spatial and Temporal memory safety.
  - Revocation is immediate.
  - Use-after-free deterministicly trapped.



- **Level 3**:
  Spatial and temporal safety (with revocation accelerated via hardware to allow immediate revocation).
  Use-after-free deterministically trapped.

- **Level 2**:
  Concurrent Temporal Safety.
  Protecting against use-after-reuse can be done without a stop-the-world phase.
  Software is assisted or accelerated by specific hardware. Revocation happens concurrently with normal execution.
  Revocation is not immediate, use after free is *not* guaranteed to trap, but an allocator can prevent use after reuse.

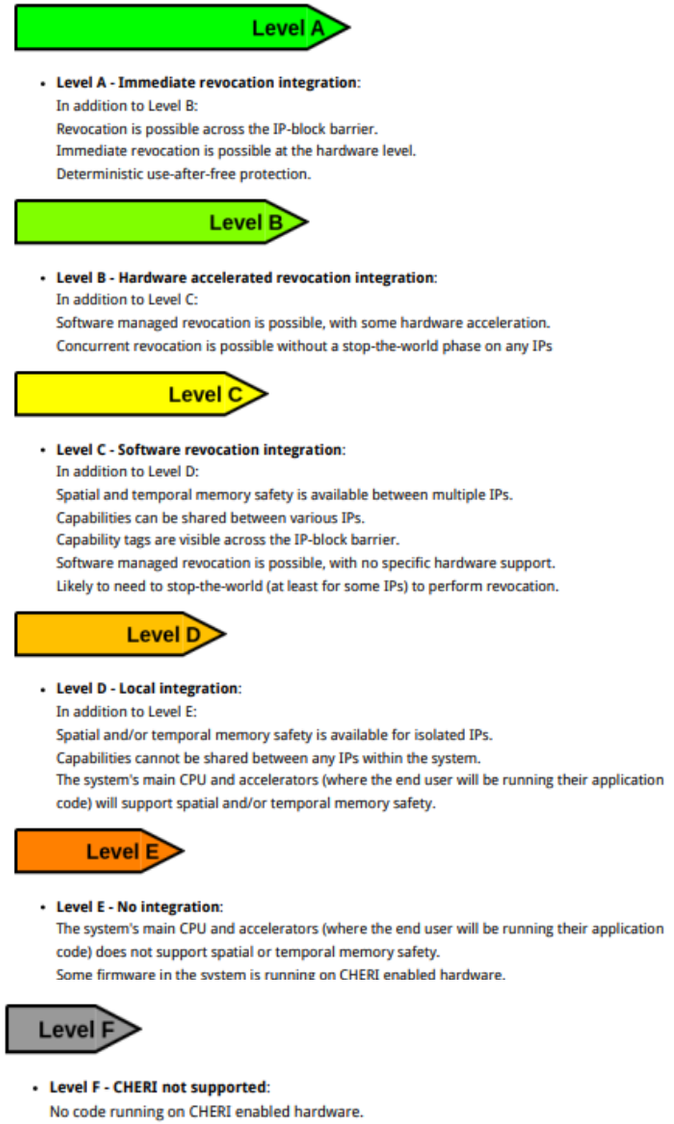
- **Level 1**:
  Basic spatial safety support.
  Spatial memory safety with bounds and permissions is supported by the IP.
  Temporal safety is possible only with a stop-the-world phase.

- **Level 0**:
  No CHERI support (i.e. legacy hardware).
  This means all memory operations are done in the regular way.
  The compiler may still make some memory-safety guarantees but these are not visible nor enforced by the hardware.

CHERI

6 levels of System Support

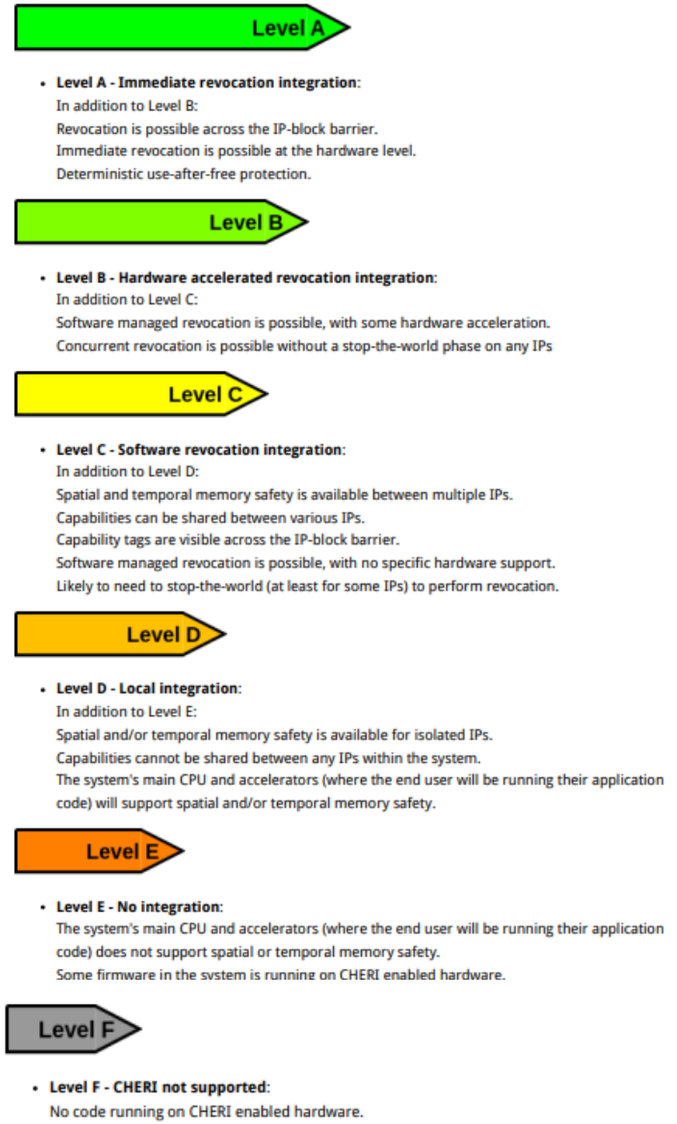
- Level F:
  - CHERI is not supported



CHERI

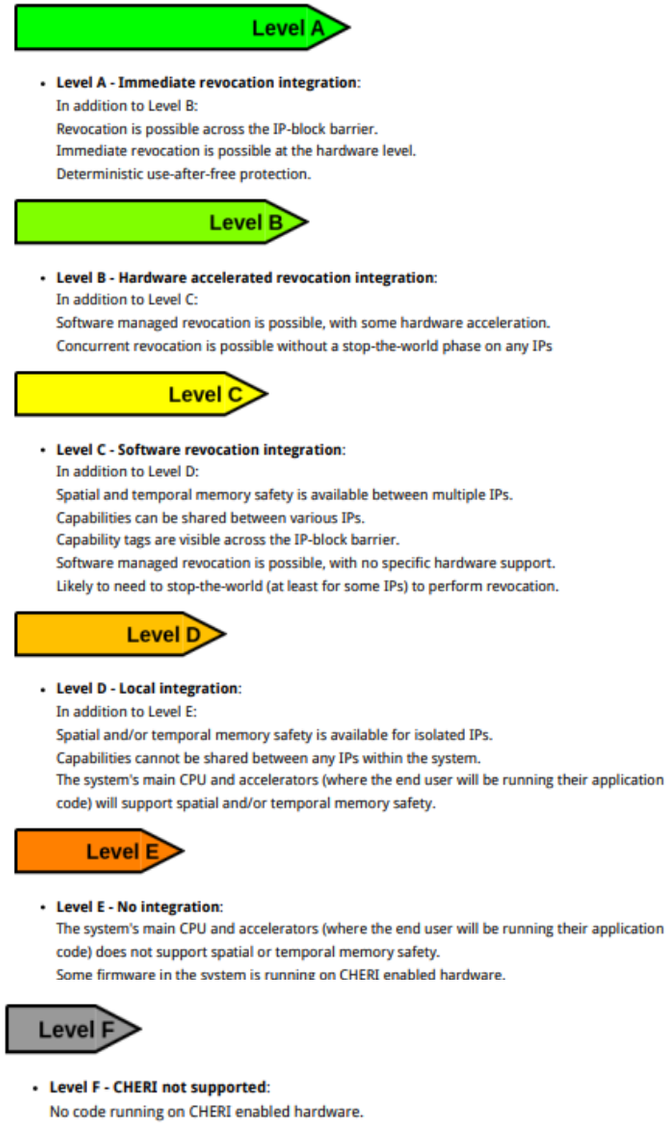
4 levels of System Support

- Level E:
  - System’s main CPU and accelerators do ***not*** support CHERI.
  - Some code on the system is running on CHERI enabled hardware.



4 levels of System Support

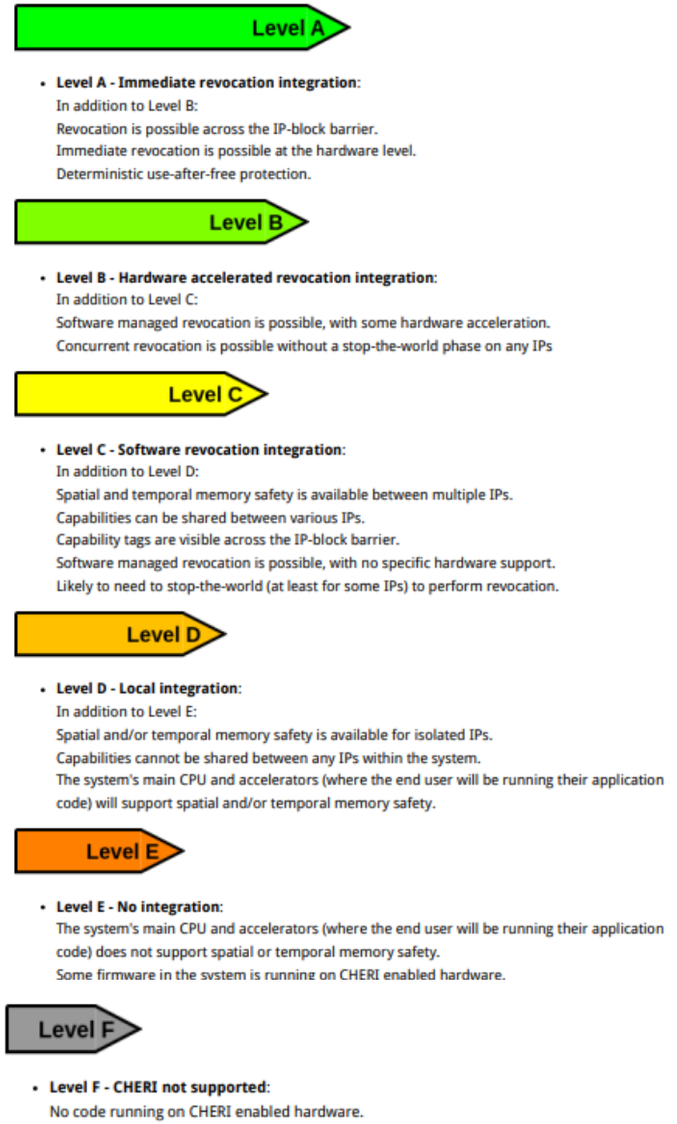
- Level D:
  - System’s main CPU and accelerators do support CHERI.



CHERI

4 levels of System Support

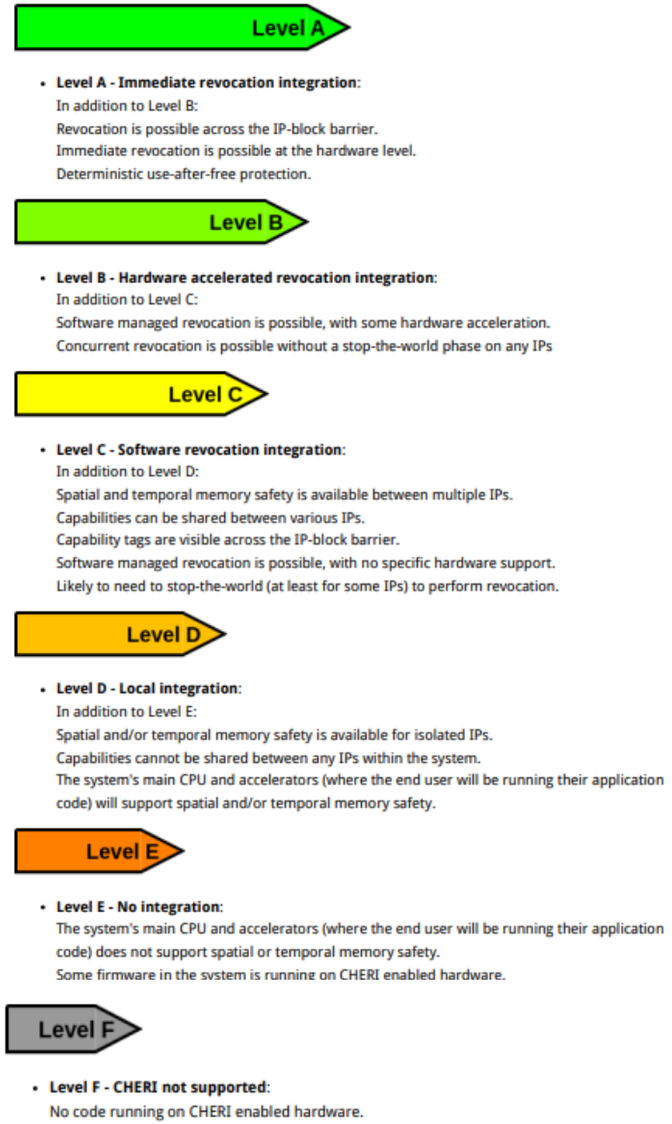
- Level C:
  - Capabilities (and tags) can be shared between multiple IPs.
  - Revocation performed using a stop-the-world phase.



CHERI

4 levels of System Support

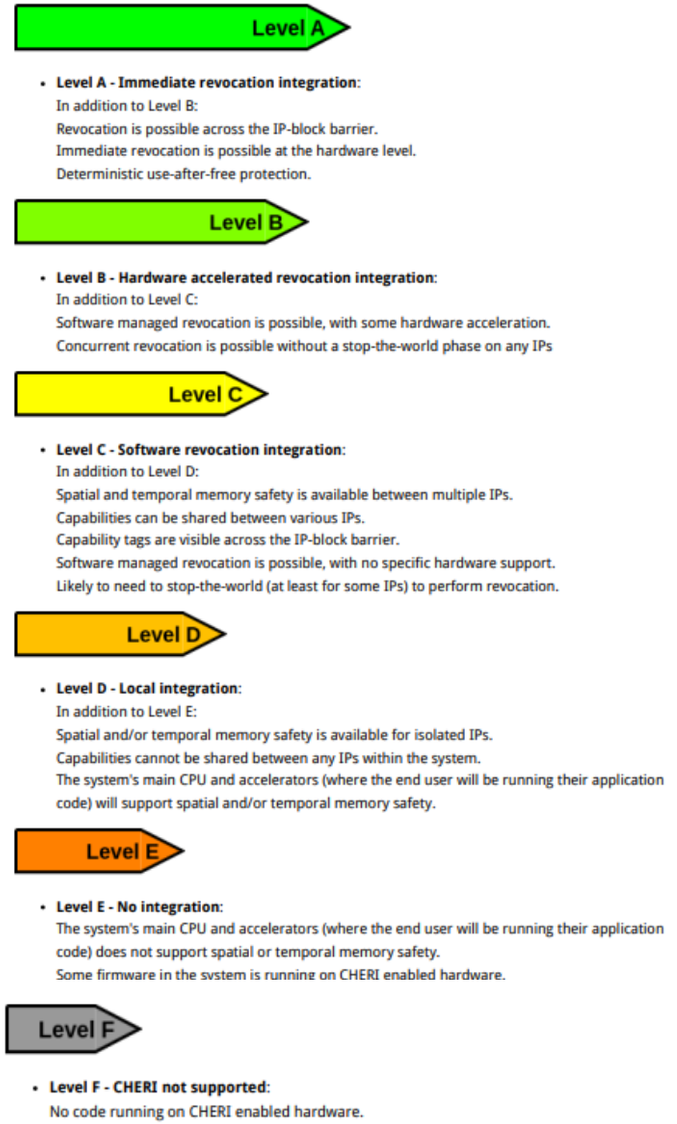
- Level B:
  - Concurrent revocation is possible without a stop-the-world phase on any IPs.



CHERI

4 levels of System Support

- Level A:
  - Revocation is possible across the IP-block barrier.
  - Immediate revocation is possible at the hardware level.
  - Deterministic use-after-free protection.



CHERI

CHERI

THANKYOU

Contact contact@cheri-alliance.org

Web www.cheri-alliance.org