Bricking

According to Wikipedia, many systems suffer from "bricking," which is when a computer is rendered no longer functional due to corrupted firmware, a hardware problem, or other damage.

This issue will be particularly dangerous on my system, because user programs have direct control over the hardware of UM, allowing them to potentially corrupt firmware and brick the device. This is why we need to have a very reliable factory reset procedure.

A simple preemption of bricking is to back up all writable firmware. Then a factory reset would clear all memory, volatile and nonvolatile, and restore the original firmware.
From the Wikipedia https://en.wikipedia.org/wiki/Brick_(electronics): "Some devices include a backup copy of their firmware, stored in fixed ROM or writable non-volatile memory, which is not normally accessible to processes that could corrupt it. Should the firmware become corrupted, the device can copy from the backup memory to its main memory, restoring the firmware."