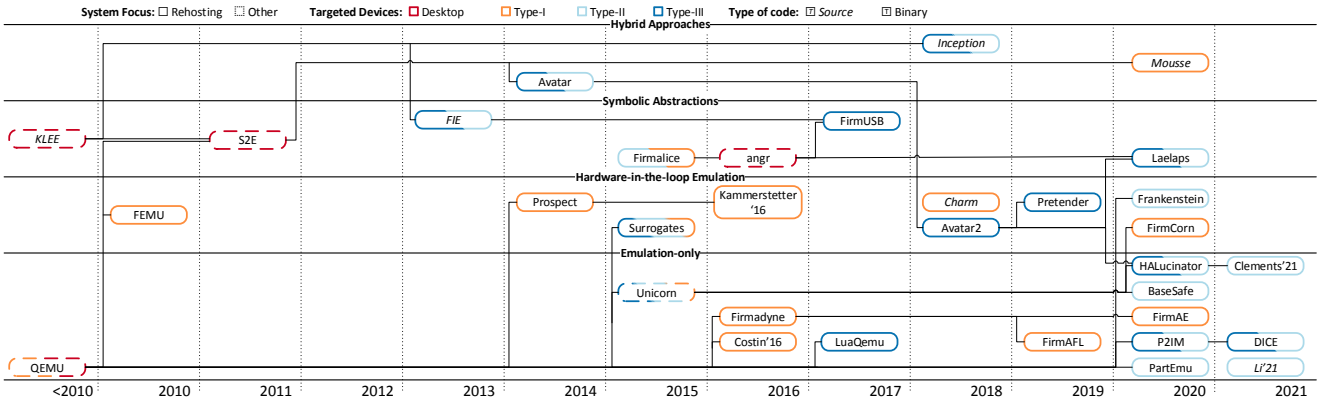

Figure 5: Timeline of Rehosting Systems.

Table 6: Total Peripherals Supported by QEMU.

Arch	v2.11.1 Total	v4.2.0 Total	v5.2.0 Total
ARM	227	321	337
ARM64	279	322	338
MIPS	153	186	192
PPC	160	210	216

add support for multiple Cortex-A9 peripherals (GIC, SCU, timers, etc.).

B.4 Aside: Peripheral Support across QEMU Versions

Looking at three major versions of QEMU approximately a year apart, v2.11.1 (February 2018, latest in Ubuntu 18.04 repositories), v4.2.0 (December 2019), and v5.2.0 (December 2020), Table 6 shows very little increase relative to corpus peripheral diversity (see Table 2 in § 4).

Regardless of which QEMU version we contrast § 4 results against, the outcome is the same. Modern QEMU is not meaningfully more capable of emulating embedded systems than it was 2.5 years ago. Despite the increasing attention the research community has given rehosting, on the HES front there has been no meaningful change. Our Monte Carlo simulation demonstrated the problem of robust peripheral support is intractable going forward, historical data complements this conclusion by demonstrating an insignificant rate of support increase.

C HISTORICAL TAXONOMY OF PRIOR WORK

Table 4 does not capture temporal or evolutionary relationships between prior work. Toward this end, we present a timeline of rehosting solutions and rehosting-related work in Fig. 5. Note that target system type, source dependecy, and primary goal (rehosting or other) are encoded in the figure.