

Emulátor ARMv6 procesoru pro emulaci prostředí Raspberry Pi

Bc. Jakub Šilhavý

vedoucí práce: Ing. Martin Úbl

Katedra informatiky a výpočetní techniky
Fakulta aplikovaných věd
Západočeská univerzita v Plzni

17. 06. 2024

Cíl práce

- návrh a implementace emulátoru platformy **Raspberry Pi Zero**
 - emulace instrukcí procesoru ARM1176JZF-S (ARMv6)
 - emulace základních periférií μ C BCM2835 (GPIO, MiniUART, BSC, ...)

① vzdělávací účely

- vizualizace principů OS
- embedded vývoj

② testování a ladění SW

③ prototypování HW

- připojení externích periférií
- návrh vlastního systému



Figure 1: Raspberry Pi Zero

- použití **KIV-RTOS** pro ověření správnosti výsledného emulátoru

- vhodné pro seznámení se s programováním v assembly
 - vizualizace, ladění programu
- floating-point instrukce
- platformová nezávislost

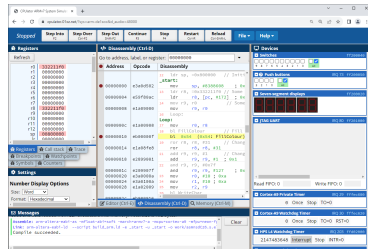


Figure 2: CPULator

Omezení

- emulace pouze CPU (ne celého SoC)
- minimální podpora pokročilých systémových operací
 - ⇒ nevhodné pro testování principů OS
- limitovaná podpora připojení externích periférií

- podpora různých architektur
 - x86, MIPS, ARM, ...
- připojení externího debuggeru
- plná podpora systémových operací



Figure 3: ► QEMU

Omezení

- emulace pouze CPU (ne celého SoC)
- limitovaná podpora připojení externích periférií
- `_start` symbol očekáván na adrese `0x00010000`
 - → nekompatibilita s *first-stage* BL Rpi0 (`0x00008000`)
- problémy se `systemtimer`

ARM1176JZF-S

- ARMv6 instrukce
- přepínání režimů CPU
- ALU, MAC a MMU
- vyjímky a přerušení
- podpora ko-procesorů
 - CP15, CP10
- systémová sběrnice

BCM2835

- RAM
- Interrupt Controller
- ARM timer
- TRNG
- GPIO
- BSC_1 (I²C)
- AUX (MiniUART)

- cílem bylo emulovat nejčastěji používané periferie
- dekompoziční návrh architektury
 - → jednoduché doimplementování dalších periférií

- jednotné rozhraní pro externí periferie
 - → připojeny přes GPIO
- nezávislé na toolchainu jádra emulátoru
- načtené při inicializaci jako sdílené knihovny (.dll, .so)

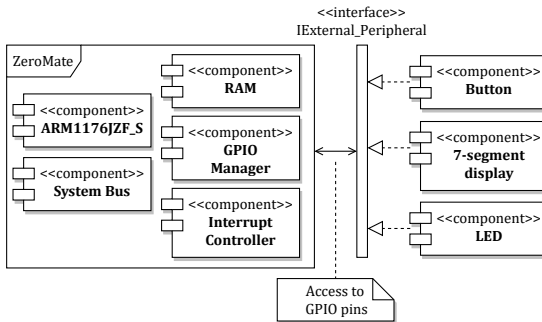


Figure 4: Rozhraní externích periferií

ZeroMate - uživatelské rozhraní

ZeroMate - Rpi Zero emulator

File Control

Step Run Stop

Reset

State: stopped

CPU Registers CP15

CPU Mode: System

USR/SYS FIQ SVC ABT IRQ UDN

HEX U32 S32

Register Value

R0	00000001
R1	00000000
R2	00000001
R3	000002BF
R4	00000004
R5	0000CE4C
R6	0000CE58
R7	00000040
R8	0000CE24
R9	0000B854
R10	00000000
R11	00004F40
R12	200000DF
R13 (LR)	00000010
R14 (SP)	00004F34
R15 (PC)	0000001C
CPSR	2000005F

Flags in CPSR

N Z C V A I F

0 0 1 0 0 0 1

Source Code Disassembly

0x0000CFFC	0xEAFFFFF4	b #0xcfd4
0x0000D000	0xE3A02001	mov r2, #1
0x0000D004	0xE59F104C	ldr r1, [pc, #0x4c]
0x0000D008	0xE5180008	ldr r0, [fp, #-8]
0x0000D00C	0xEB000145	bl #0xd528
0x0000D010	0xE3A03000	mov r3, #0
0x0000D014	0xE50B300C	str r3, [fp, #-0xc]
0x0000D018	0xE518300C	ldr r3, [fp, #-0xc]
0x0000D01C	0xE3536001	cmp r3, #0x400
0x0000D020	0xB3A03001	movlt r3, #1
0x0000D024	0xA3A03000	movge r3, #0
0x0000D028	0xE6EF3073	uxtb r3, r3
0x0000D02C	0xE3530000	cmp r3, #0
0x0000D030	0x0AFFFE1	beq #0xcfc
0x0000D034	0xE51B300C	ldr r3, [fp, #-0xc]
0x0000D038	0xE2833001	add r3, r3, #1
0x0000D03C	0xE50B300C	str r3, [fp, #-0xc]
0x0000D040	0xEAFFFFF4	b #0xd018
0x0000D044	0x0000E11C	andeq lr, r0, ip, lsl r1
0x0000D048	0x0000E128	andeq lr, r0, r8, lsr #2

RAM GPIO IC ARM timer Monitor

Debug monitor: 80x25 8-bit characters

```

1: finding child = segd
2: child was not found
3: creating: segd
4: Finished FS initialization
5:
6: Created process with pid 1 (SP = 0x24000)
7: Created process with pid 2 (SP = 0x28000)
8: Created process with pid 3 (SP = 0x2C000)
9: Created process with pid 4 (SP = 0x30000)
10: Created process with pid 5 (SP = 0x34000)
11: opening file: DEV:segd
12: process 5 file descriptor = 0
13: opening file: DEV:gpio/20
14: process 4 file descriptor = 0
15: opening file: DEV:gpio/19
16: process 3 file descriptor = 0
17: opening file: DEV:monitor/0
18: opening file: DEV:trng
19: process 2 file descriptor (f) = 0
20: process 2 file descriptor (rndf) = 1
21: 418294306opening file: DEV:gpio/18
22: process 1 file descriptor = 0
23: 2562694996194938438940474621931554527732535076234846925.
24: 4860613283457108318681854161190600104478572298110939180
25: 01381446152226272834524632757932711601301463

```

Logs

Options Clear Copy Filter

```

[debug][control_window.cpp:200] CPU execution has stopped
[warning][core.cpp:367] IRQ exception
[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled
[warning][core.cpp:367] IRQ exception
[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled
[warning][core.cpp:367] IRQ exception
[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled
[info][control_window.cpp:200] CPU execution has stopped

```

The screenshot displays the ZeroMate - Rpi Zero emulator interface. The main window is divided into several panels:

- File Control:** Includes buttons for Step, Run, and Stop. The state is "stopped".
- CPU Registers:** Shows the CPU Mode as System and various registers (USR/SYS, FIQ, SVC, ABT, IRQ, UDN). The selected register is U32, showing a value of 00000001.
- Source Code Disassembly:** Displays assembly code for the ARM processor. The current instruction is "cmp r3, #0x400" at address 0x0000001C.
- RAM:** Shows the memory dump starting from address 0x00000000.
- GPIO IC ARM timer Monitor:** Displays the debug monitor output, showing the sequence of events from finding the child to opening files.
- Logs:** Shows the execution logs, including warnings and debug messages.

A tooltip is visible over the "SOS btn" button, indicating "GPIO pin: 16" and "Press".

ZeroMate - externí periferie

The screenshot displays the ZeroMate - Rpi Zero emulator interface. The main window is divided into several panels:

- File Control:** Includes buttons for Step, Run, and Stop. The state is "stopped".
- CPU Registers:** Shows the CPU Mode as System. The register list includes USR/SYS, FIQ, SVC, ABT, IRQ, and UDN. The register values are listed in a table.
- Source Code Disassembly:** Displays assembly code for the ARM processor. The current instruction is `cmp r3, #0x400` at address `0x0000001C`.
- RAM:** Shows the memory address `0x0000001C` and the value `0x0000001C`.
- Debug Monitor:** Displays the debug output, including the text "My favourite sport is ARM wrestling" on the SSD1306 OLED display.
- Logs:** Shows a list of log messages, including "Basic IRQ ARM_Timer has been signaled" and "CPU execution has stopped".

Overlaid on the right side of the emulator window are two UI elements:

- A blue button labeled "SOS btn" with a "Press" label below it.
- A text box displaying "GPIO pin: 16".

ZeroMate - externí periferie

ZeroMate - Rpi Zero emulator

File Control

Step Run Stop

Reset

State: stopped

CPU Registers CP15

CPU Mode: System

USR/SYS FIQ SVC ABT IRQ UDN

HEX U32 S32

Register Value

R0 00000001

R1 00000000

R2 00000001

R3 0000028F

R4 00000004

R5 0000CE4C

R6 0000CE50

R7 00000040

R8 0000CE24

R9 0000B854

R10 00000000

R11 00004F40

R12 2000000F

R13 (LR) 00000010

R14 (SP) 00004F34

R15 (PC) 0000001C

CPSPR 2000005F

Flags in CPSR

N Z C V A I F

0 0 1 0 0 0 1

Source Code Disassembly

0x0000CFFC 0xEAFFFFF4 b #0xcfd4

0x0000D000 0xE3A02001 mov r2, #1

0x0000D004 0xE59F104C ldr r1, [pc, #0x4c]

0x0000D008 0xE5180008 ldr r0, [fp, #-8]

0x0000D00C 0xEB000145 bl #0xd528

0x0000D010 0xE3A03000 mov r3, #0

0x0000D014 0xE50B300C str r3, [fp, #-0xc]

0x0000D018 0xE51B300C ldr r3, [fp, #-0xc]

0x0000D01C 0xE3530B01 cmp r3, #0x400

0x0000D020 0xB3A03001 movlt r3, #1

0x0000D024 0xA3A03000 movge r3, #0

0x0000D028 0xE6EF3073 uxtb r3, r3

0x0000D02C 0xE3530000 cmp r3, #0

0x0000D030 0x0AFFFE1 beq #0xcfb

0x0000D034 0xE51B300C ldr r3, [fp, #-0xc]

0x0000D038 0xE2833001 add r3, r3, #1

0x0000D03C 0xE50B300C str r3, [fp, #-0xc]

0x0000D040 0xEAFFFFF4 b #0xd018

0x0000D044 0x0000E11C andeq lr, r0, ip, lsl r1

0x0000D048 0x0000E128 andeq lr, r0, r8, lsr r1

Logs

Options Clear Copy

[warning][core.cpp:367] IRQ exception

[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled

[warning][core.cpp:367] IRQ exception

[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled

[warning][core.cpp:367] IRQ exception

[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled

[info][control_window.cpp:200] CPU execution has stopped

RAM GPIO IC ARM timer Monitor

Debug monitor: 80x25 8-bit characters

1: finding child = segd

2: child was not found

3: creating: segd

4: Finished FS initialization

5:

6: Created process with pid 1 (SP = 0x20000)

7: Created process with pid 2 (SP = 0x20000)

8:

9:

10:

11:

12:

13:

14:

15:

16:

17:

18:

19:

20:

21:

22:

23:

24:

25:

26:

27:

28:

29:

30:

31:

32:

33:

34:

35:

36:

37:

38:

39:

40:

41:

42:

43:

44:

45:

46:

47:

48:

49:

50:

51:

52:

53:

54:

55:

56:

57:

58:

59:

60:

61:

62:

63:

64:

65:

66:

67:

68:

69:

70:

71:

72:

73:

74:

75:

76:

77:

78:

79:

80:

81:

82:

83:

84:

85:

86:

87:

88:

89:

90:

91:

92:

93:

94:

95:

96:

97:

98:

99:

100:

101:

102:

103:

104:

105:

106:

107:

108:

109:

110:

111:

112:

113:

114:

115:

116:

117:

118:

119:

120:

121:

122:

123:

124:

125:

126:

127:

128:

129:

130:

131:

132:

133:

134:

135:

136:

137:

138:

139:

140:

141:

142:

143:

144:

145:

146:

147:

148:

149:

150:

151:

152:

153:

154:

155:

156:

157:

158:

159:

160:

161:

162:

163:

164:

165:

166:

167:

168:

169:

170:

171:

172:

173:

174:

175:

176:

177:

178:

179:

180:

181:

182:

183:

184:

185:

186:

187:

188:

189:

190:

191:

192:

193:

194:

195:

196:

197:

198:

199:

200:

201:

202:

203:

204:

205:

206:

207:

208:

209:

210:

211:

212:

213:

214:

215:

216:

217:

218:

219:

220:

221:

222:

223:

224:

225:

226:

227:

228:

229:

230:

231:

232:

233:

234:

235:

236:

237:

238:

239:

240:

241:

242:

243:

244:

245:

246:

247:

248:

249:

250:

251:

252:

253:

254:

255:

256:

257:

258:

259:

260:

261:

262:

263:

264:

265:

266:

267:

268:

269:

270:

271:

272:

273:

274:

275:

276:

277:

278:

279:

280:

281:

282:

283:

284:

285:

286:

287:

288:

289:

290:

291:

292:

293:

294:

295:

296:

297:

298:

299:

300:

301:

302:

303:

304:

305:

306:

307:

308:

309:

310:

311:

312:

313:

314:

315:

316:

317:

318:

319:

320:

321:

322:

323:

324:

325:

326:

327:

328:

329:

330:

331:

332:

333:

334:

335:

336:

337:

338:

339:

340:

341:

342:

343:

344:

345:

346:

347:

348:

349:

350:

351:

352:

353:

354:

355:

356:

357:

358:

359:

360:

361:

362:

363:

364:

365:

366:

367:

368:

369:

370:

371:

372:

373:

374:

375:

376:

377:

378:

379:

380:

381:

382:

383:

384:

385:

386:

387:

388:

389:

390:

391:

392:

393:

394:

395:

396:

397:

398:

399:

400:

401:

402:

403:

404:

405:

406:

407:

408:

409:

410:

411:

412:

413:

414:

415:

416:

417:

418:

419:

420:

421:

422:

423:

424:

425:

426:

427:

428:

429:

430:

431:

432:

433:

434:

435:

436:

437:

438:

439:

440:

441:

442:

443:

444:

445:

446:

447:

448:

449:

450:

451:

452:

453:

454:

455:

456:

457:

458:

459:

460:

461:

462:

463:

464:

465:

466:

467:

468:

469:

470:

471:

472:

473:

474:

475:

476:

477:

478:

479:

480:

481:

482:

483:

484:

485:

486:

487:

488:

489:

490:

491:

492:

493:

494:

495:

496:

497:

498:

499:

500:

501:

502:

503:

504:

505:

506:

507:

508:

509:

510:

511:

512:

513:

514:

515:

516:

517:

518:

519:

520:

521:

522:

523:

524:

525:

526:

527:

528:

529:

530:

531:

532:

533:

534:

535:

536:

537:

538:

539:

540:

541:

542:

543:

544:

545:

546:

547:

548:

549:

550:

551:

552:

553:

554:

555:

556:

557:

558:

559:

560:

561:

562:

563:

564:

565:

566:

567:

568:

569:

570:

571:

572:

573:

574:

575:

576:

577:

578:

579:

580:

581:

582:

583:

584:

585:

586:

587:

588:

589:

590:

591:

592:

593:

594:

595:

596:

597:

598:

599:

600:

601:

602:

603:

604:

605:

606:

607:

608:

609:

610:

611:

612:

613:

614:

615:

616:

617:

618:

619:

620:

621:

622:

623:

624:

625:

626:

627:

628:

629:

630:

631:

632:

633:

634:

635:

636:

637:

638:

639:

640:

641:

642:

643:

644:

645:

646:

647:

648:

649:

650:

651:

652:

653:

654:

655:

656:

657:

658:

659:

660:

661:

662:

663:

664:

665:

666:

667:

668:

669:

670:

671:

672:

673:

674:

675:

676:

677:

678:

679:

680:

681:

682:

683:

684:

685:

686:

687:

688:

689:

690:

691:

692:

693:

694:

695:

696:

697:

698:

699:

700:

701:

702:

703:

704:

705:

706:

707:

708:

709:

710:

711:

712:

713:

714:

715:

716:

717:

718:

719:

720:

721:

722:

723:

724:

725:

726:

727:

728:

729:

730:

731:

732:

733:

734:

735:

736:

737:

738:

739:

740:

741:

742:

743:

744:

745:

746:

747:

748:

749:

750:

751:

752:

753:

754:

755:

756:

757:

758:

759:

760:

761:

762:

763:

764:

765:

766:

767:

768:

769:

770:

771:

772:

773:

774:

775:

776:

777:

778:

779:

780:

781:

782:

783:

784:

785:

786:

787:

788:

789:

790:

791:

792:

793:

794:

795:

796:

797:

798:

799:

800:

801:

802:

803:

804:

805:

806:

807:

808:

809:

810:

811:

812:

813:

814:

815:

816:

817:

818:

819:

820:

821:

822:

823:

824:

825:

826:

827:

828:

829:

830:

831:

832:

833:

834:

835:

836:

837:

838:

839:

840:

841:

842:

843:

844:

845:

846:

847:

848:

849:

850:

851:

852:

853:

854:

855:

856:

857:

858:

859:

860:

861:

862:

863:

864:

865:

866:

867:

868:

869:

870:

871:

872:

873:

874:

875:

876:

877:

878:

879:

880:

881:

882:

883:

884:

885:

886:

887:

888:

889:

890:

891:

892:

893:

894:

895:

896:

897:

898:

899:

900:

901:

902:

903:

904:

905:

906:

907:

908:

909:

910:

911:

912:

913:

914:

915:

916:

917:

918:

919:

920:

921:

922:

923:

924:

925:

926:

927:

928:

929:

930:

931:

932:

933:

934:

935:

936:

937:

938:

939:

940:

941:

942:

943:

944:

945:

946:

947:

948:

949:

950:

951:

952:

953:

954:

955:

956:

957:

958:

959:

960:

961:

962:

963:

964:

965:

966:

967:

968:

969:

970:

971:

972:

973:

974:

975:

976:

977:

978:

979:

980:

981:

982:

983:

984:

985:

986:

987:

988:

989:

990:

991:

992:

993:

994:

995:

996:

997:

998:

999:

1000:

1001:

1002:

1003:

1004:

1005:

1006:

1007:

1008:

1009:

1010:

1011:

1012:

1013:

1014:

1015:

1016:

1017:

1018:

1019:

1020:

1021:

1022:

1023:

1024:

1025:

1026:

1027:

1028:

1029:

1030:

1031:

1032:

1033:

1034:

1035:

1036:

1037:

1038:

1039:

1040:

1041:

1042:

1043:

1044:

1045:

1046:

1047:

1048:

1049:

1050:

1051:

1052:

1053:

1054:

1055:

1056:

1057:

1058:

1059:

1060:

1061:

1062:

1063:

1064:

1065:

1066:

1067:

1068:

1069:

1070:

1071:

1072:

1073:

1074:

1075:

1076:

1077:

1078:

1079:

1080:

1081:

1082:

1083:

1084:

1085:

1086:

1087:

1088:

1089:

1090:

1091:

1092:

1093:

1094:

1095:

1096:

1097:

1098:

1099:

1100:

1101:

1102:

1103:

1104:

1105:

1106:

1107:

1108:

1109:

1110:

1111:

1112:

1113:

1114:

1115:

1116:

1117:

1118:

1119:

1120:

1121:

1122:

1123:

1124:

1125:

1126:

1127:

1128:

1129:

1130:

1131:

1132:

1133:

1134:

1135:

1136:

1137:

1138:

1139:

1140:

1141:

1142:

1143:

1144:

1145:

1146:

1147:

1148:

1149:

1150:

1151:

1152:

1153:

1154:

1155:

1156:

1157:

1158:

1159:

1160:

1161:

1162:

1163:

1164:

1165:

1166:

1167:

1168:

1169:

1170:

1171:

1172:

1173:

1174:

1175:

The screenshot displays the ZeroMate - Rpi Zero emulator interface, which is divided into several panels:

- File Control:** Includes buttons for Step, Run, and Stop, a Reset button, and a State indicator showing "stopped".
- CPU Registers:** Shows the CPU Mode as System and a list of registers (R0-R15, CPSR) with their values. The R15 (PC) register is highlighted.
- Source Code Disassembly:** Displays assembly code for the program. The instruction at address 0x0000001C, "cmp r3, #0x400", is highlighted.
- RAM:** Shows the memory address 0x0000001C and the value 0x00000000.
- GPIO IC:** Shows the GPIO pin configuration. The S0S btn is connected to GPIO pin 16, and the S0S LED is connected to GPIO pin 18.
- ARM timer:** Shows the timer configuration. The timer is set to 1000 Hz.
- Monitor:** Displays the output of the program. The text "My favourite sport is ARM wrestling" is shown on the SSD1306 OLED display. The 7-segment display shows the number "8".
- Logs:** Shows the execution logs, including warnings about IRQ exceptions and the CPU execution has stopped message.

Overlaid on the emulator interface are several callouts:

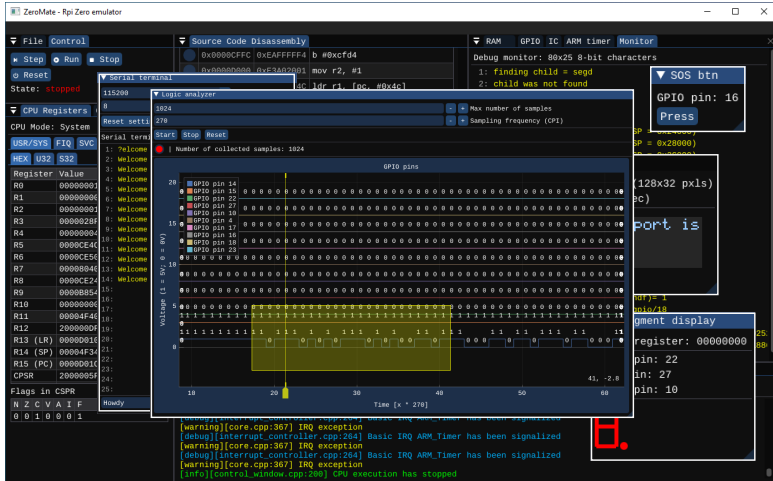
- A blue box labeled "S0S btn" with a "Press" button, indicating the button press event.
- A green box labeled "S0S LED" with a green circle and "Color" text, indicating the LED state.
- A red box labeled "7-segment display" showing the number "8", indicating the display output.

ZeroMate - externí periferie

The screenshot displays the ZeroMate - Rpi Zero emulator interface, which is divided into several panels:

- File/Control:** Includes buttons for Step, Run, Stop, and Reset. The state is "stopped".
- CPU Registers:** Shows the CPU Mode (System) and registers R0 through R15, along with CPSR. The register values are mostly 00000000, except for R15 (PC) which is 2000005F.
- Serial terminal:** Displays a message "115200" and a list of "Welcome to KIV/OS RPiOS kernel" messages for each register.
- Source Code Disassembly:** Shows assembly code for the ARM processor, including instructions like "mov r2, #1", "ldr r1, [pc, #0x4c]", "ldr r0, [fp, #-8]", "bl #0xd528", "mov r3, #0", "str r3, [fp, #-0xc]", "ldr r3, [fp, #-0xc]", "cmp r3, #0x400", "movlt r3, #1", "movge r3, #0", "uxtb r3, r3", "cmp r3, #0", "beq #0xcfb", "ldr r3, [fp, #-0xc]", "add r3, r3, #1", "str r3, [fp, #-0xc]", "b #0xd018", "andeq lr, r0, ip, lsl r", and "andeq lr, r0, r8, lsr #".
- RAM:** Shows the debug monitor output, including "finding child = segd", "child was not found", "creating: segd", "Finished FS initialization", "Created process with pid 1 (SP = 0x20000)", "Created process with pid 2 (SP = 0x20000)", "SSD1306 OLED", "SSD1306 OLED display (128x32 pxls)", "I2C addr = 0x3C (60 dec)", "My favourite sport is ARM wrestling", "process 2 file descriptor (rmr) = 1", "416294986Opening file: /dev/gpio/18", "7-segment display", "shift register: 00000000", "Latch pin: 22", "Data pin: 27", "Clock pin: 10", and "GPIO pin: 16".
- GPIO IC ARM timer Monitor:** Shows a "SOS btn" button and a "SOS LED" indicator.
- Console:** Displays a series of log messages, including "[debug][interrupt_controller.cpp:264] Basic IRQ ARM_Timer has been signaled", "[warning][core.cpp:367] IRQ exception", and "[info][control_window.cpp:200] CPU execution has stopped".

ZeroMate - externí periferie



Děkuji Vám za pozornost

► <https://github.com/silhavyj/ZeroMate>

