The Wild and Wonderful World of 8-bit microprocessors with a focus on the MOS6502

Michael R. Brown

Hardware Hacking Village @ Defcon 2024

Bio- Michael R. Brown

- BS & MCS @ FAU- Software Engineering
- 20+ years in IT, last half in InfoSec
- Unix (Sun/Solaris, HP-UX, AIX) SysAdmin, Windows/AD SysAdmin
- Part of an IT org assessed at CMM Level 3.
- Security Admin for global company from local level to global level.
- Global Security Architect, part of CISO's team of a global company.
- Security Consultant in area of Governance, Risk, Compliance, & a vCISO.
- Now Security & Compliance Director focused on HITRUST & SOC 1/2.
- Experience with HIPAA-HITECH, ISO/IEC 27001, NIST CSF, CIS Controls, SOC 2, PCI-DSS, HITRUST, CMMC, etc.
- Active with ISSA (SoFL chapter), Infragard, ISACA, ISC(2), IAPP, etc.

Background relating to topic

- Grew up in era of Apple II, Atari 8-bit, Commodore 8-bit
- First game console was Atari 2600 ~78/79
- First computer was Atari 800XL ~1984
  - Second was Atari ST 1040STfm ~1989
- Programmed in 6502 & 68000 in college (early 80s)
  - Used an HP 9836, based on 68000.





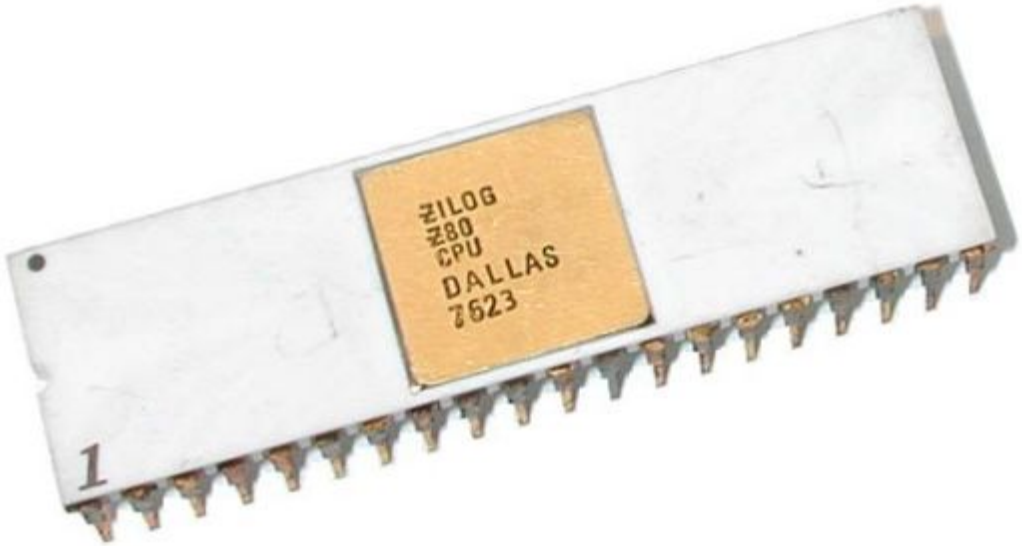


Outline

- Setting the stage- timeline & computer types
- Overview of Semiconductor companies
- Getting into MPUs
  - 6502
  - KIM-1
- Programming- high-level vs machine code/assembly
  - 6502 assembly language
- Next steps
  - Books
  - Hardware/Software
- Questions

What about the Zilog Z80??

- The Zilog Z80 was and is a popular 8-bit processor
- It was used in many 8-bit computers, game consoles, and other uses.
- Everything we say here about the 6502 is largely true of the Z80
- But due to time constraints, we will overlook it.
- Still being made until April 2024!
- Equivalent is eZ80 chip, still available



Basic timeline- the 70s

- 1974
  - Intel 8080 released
  - MITS releases Altair 8800 computer [8080 based]
  - Motorola 6800 released
- 1975
  - MOS Technology 6501& 6502 released
- 1976
  - Zilog Z80 released
- 1977
  - Atari 2600 released [6507 based]
  - Apple II released [6502 based]
  - Commodore PET released [6502 based]
  - TRS-80 Model 1 released [Z80 based]

Basic Timeline- the 80s

- 1980
  - Tandy Color Computer released [6809 based]
- 1981
  - Commodore Vic-20 released [6502 based]
  - IBM PC released [8088 based]
- 1982
  - Commodore 64 released [6510 based]
- 1984
  - Apple Macintosh released [68000 based]
  - Motorola 68020 released
- 1985
  - Atari ST released [68000 based]
  - Commodore Amiga released [68000 based]

Computer types

- Mainframe (large computers, room sized)
  - Snow White & 7 Dwarfs (IBM & Burroughs, Univac, NCR, CDC, Honeywell, RCA, GE)
  - IBM & BUNCH (Burroughs, Univac, NCR, CDC, Honeywell)
  - Today: IBM, Unisys, HPE, Hitachi, Fujitsu, Groupe Bell
- Minicomputer/midrange (small computers, refrigerator sized)
  - Digital, Data General, HP, Wang, Prime, TI, etc
- Microcomputer (CPU is a microchip)
  - MITS, IMSAI, Sol, later Apple, Atari, Commodore et al

Microcontrollers

- Microcontrollers are MCU usually restricted memory.
- Can be programmed, but not able to run an OS.
- Used to control devices (embedded systems, automotive, appliances, office machines, etc).
- Many times microprocessors can be used as microcontrollers.
  - 6502-derived items used as disk controllers, etc.

Semiconductor Manufacturers



- Shockley Semiconductor (1955-68)
  - Founder invented the transistor
- Fairchild Semiconductor (established by “traitorous 8”) (1957-2016)
  - Integrated circuit (IC) developed here and at Texas Instruments.
  - F8 microprocessor
  - Channel F video game console, first use of ROM cartridges
- Intel (founded by “fairchildren”) (est 1968)
  - 4004/4040, 8008/8080, 8086/8088, 80186 to 486, 80586/Pentium, i860 & i960, Itanium
  - Now: Atom, Celeron, Core i3/i5/i7/i9, Xeon
- Zilog (1974-2009, now subsidiary)
  - Z80, Z8000, Z80000



Semiconductor Manufacturers

- Motorola (later Freescale, now part of NXP)
  - 6800, 6809, 68000, 68020-060, 88000, PowerPC
- MOS Technology (1969-2001, NOT to be confused with Mostek, later Commodore Semiconductor Group)
  - 6501, 6502 & derivatives (65CE02), chips for Amiga etc.
- Western Design Center (est 1978)
  - 65C02, 65816





Semiconductor Manufacturers



- Texas Instruments (TI, 1930, 1951)
  - TMS9900
- National Semiconductor (1959-2011, bought by TI)
  - SC/MP, 32000 series



- There are many manufacturers who make chips but do not design them. Many are “second sources” for processors designed by other companies and may produce variants.

The PC before the IBM PC

- Many companies built these standard “business computers”
  - 8080 or Z80 based
  - S-100 bus (aka Altair bus) [an IEEE standard until the mid 90s!]
  - CP/M (CP/M-80) operating system

  - But no standard for floppy drives
    - 8in, 5.24in, soft sector, hard sector, single/double density, single/double sided

  - But so popular that 6502-based systems often has a way to add a Z80 to run CP/M and its software (Apple, Atari, Commodore, etc).
  - And is STILL popular in retro computing circles.

What makes a system 8bit? 16bit? 32bit?

- And what about 8/16bit? 16/32bit?

- And did you know there were 12bit, 24bit, 36bit, 48bit, and others computers? [tho not microprocessors]

- 64-bit?? Not TRUE = □



Characteristics of microprocessors

- Clock speed
  - MIPS is a better measurement to compare MPUs
  - 6502 is .43 and 68000 is .175!
- Address bus
  - Determines how much memory can be addressed
- Size and number of registers
- Data bus
  - Data bus for chip determines data bus for entire system. ALL components must use the same size.

IBM Personal Computer (model 5150)

- Released in 1981
- Intel 8088 microprocessor
- 16 or 64K
- 5.25 floppy drives
- Color Graphics Adapter (CGA)
- ISA bus
- MS-DOS



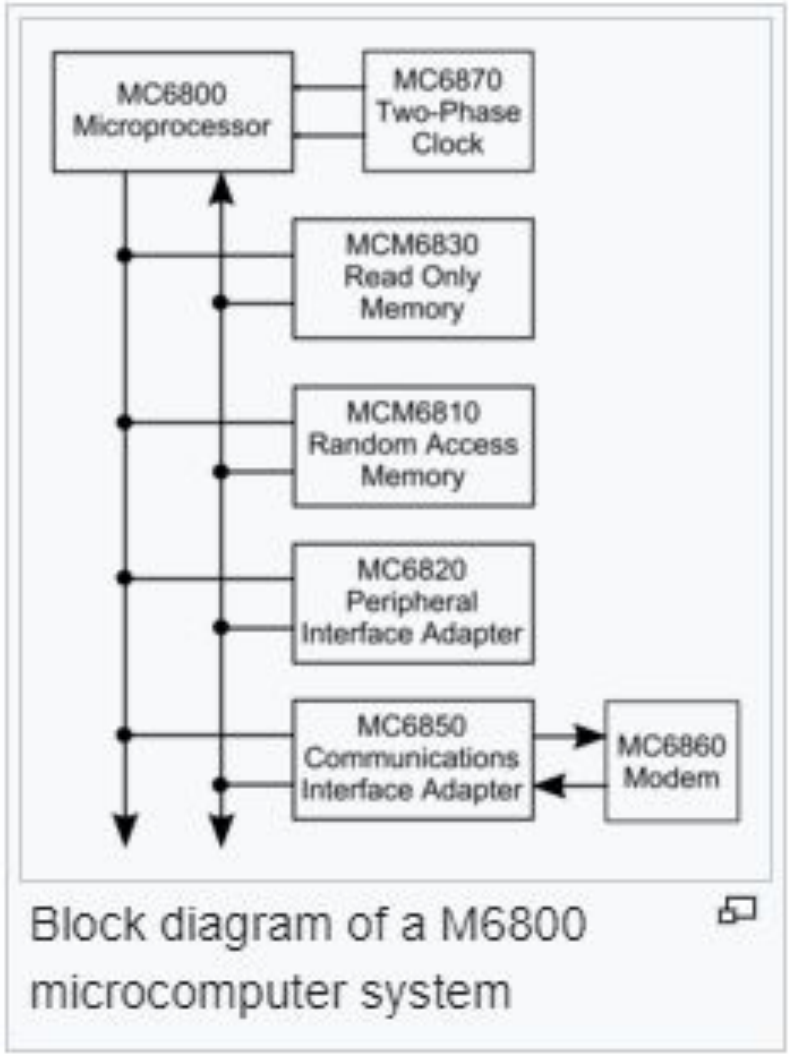
- QUESTION: was it a 16bit or 8bit computer?

Motorola 6800

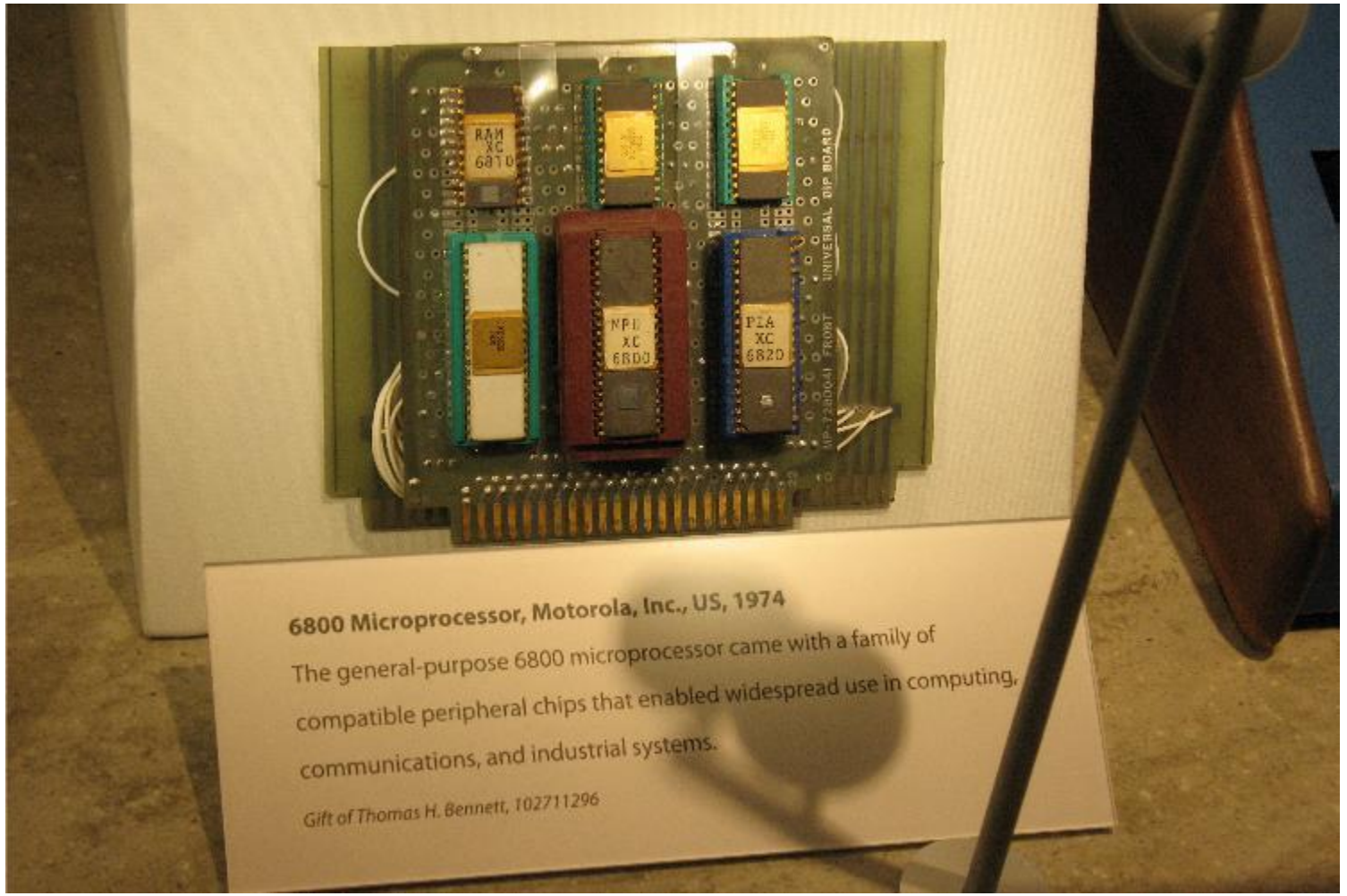
- Released in 1974
- 8bit data bus, 16bit address bus (64K)
- 72 instructions (opcode)
- 40-pin DIP
- Based on DEC PDP-11 architecture
- Part of a “total product family” of chips
- Originally cost ~$360, later reduced to $179 then to $69

- Later replaced by the more powerful 6809 (‘78), which is not opcode compatible.

6800



Block diagram of a M6800 microcomputer system



6800 vs 6502

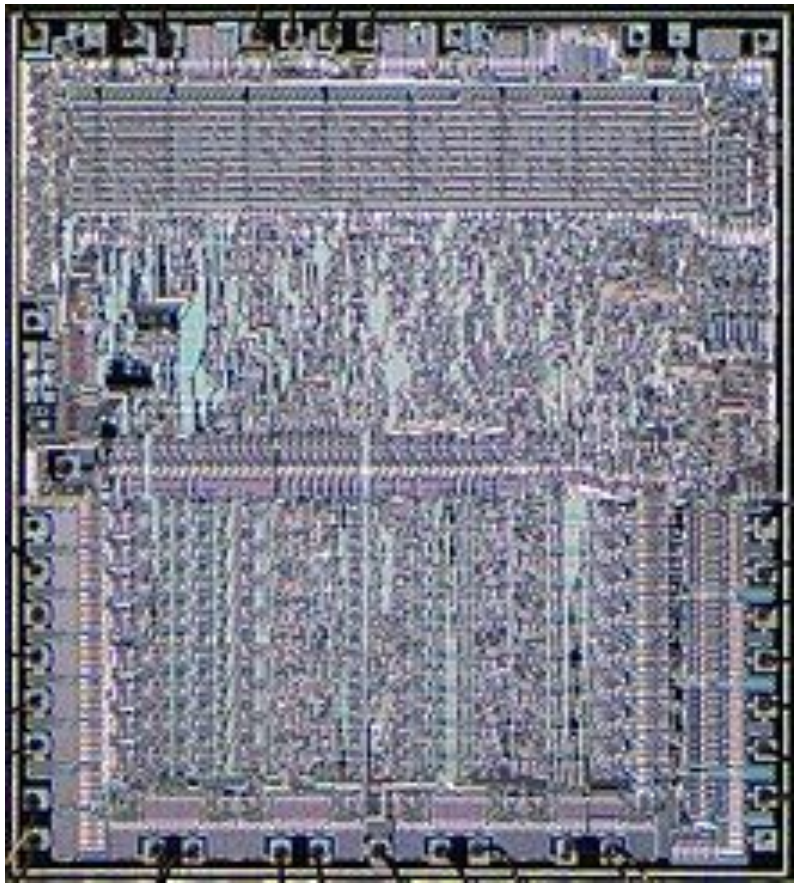
Motorola 6800 registers

15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00	*(bit position)*
Main registers																
							A									**A** accumulator
							B									**B** accumulator
Index registers																
							IX									Index register
							SP									**S**tack Pointer
Program counter																
							PC									Program Counter
Status register																
												1	1	H	I	N	Z	V	C	Flags

MOS 6502 registers

15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00	*(bit position)*
Main registers																
							A									Accumulator
Index registers																
							X									**X** index
							Y									**Y** index
0	0	0	0	0	0	0	1	SP								Stack Pointer
Program counter																
							PC									Program Counter
Status register																
												N	V	-	B	D	I	Z	C	Processor Flags

MOS Technology 6502



- Released in 1975
- 8bit data bus, 16bit address bus (64K)
- 55 instructions (opcode) [vs 77 in 6800]
- 40-pin DIP
- “cost reduced version” of 6800 to a degree
- Part of a “total product family” of chips
- Originally cost $25!!!
- Chuck Peddle lead team, Bill Mensch credited as creator or co-creator.

6502 (and variants) usage





- Acorn Atom & Electron/BBC Micro & Master
- Apple I, II, III
- Atari 2600, 5200, 7800, 400/800/XL/XE, Lynx
- Commodore PET, VIC-20, 64, 128, etc
- Famicom/Nintendo Entertainment System
- Ohio Scientic
- TurboGrafx-16
- WDC65816 8/16 processor used in:
  - Apple IIgs [designed for it]
  - SuperNES











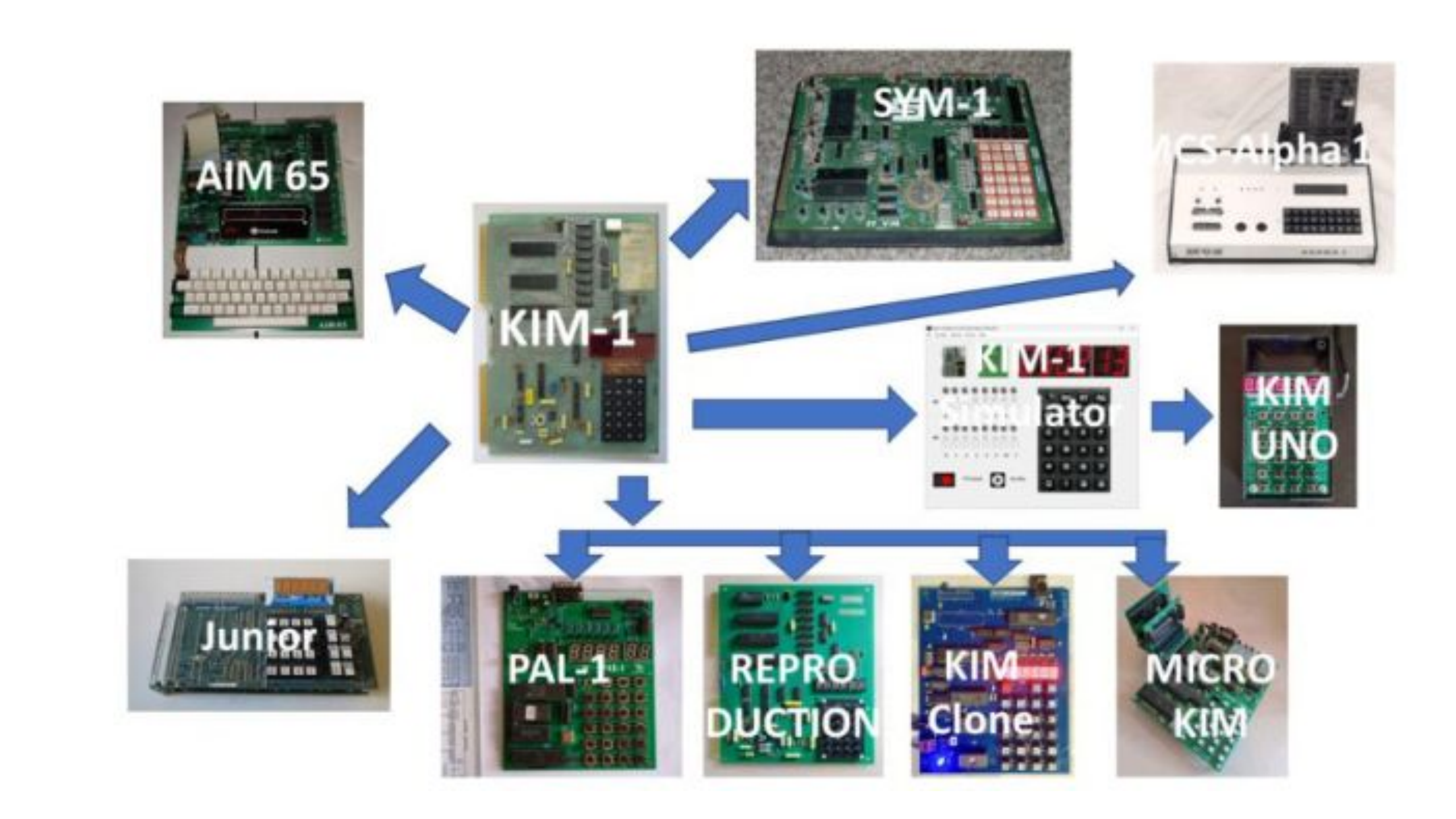




KIM-1



- Created by Chuck Peddle @ MOS
- Designed as a single-board computer to demo the 6502 to potential buyers in 1976
- Due to low cost (~$250), was popular among hobbyists
- 6502, 2 6530 PIA, ROM, 4K RAM, 7 alpha-numeric LEDs, 24key pad
- Expansion port to add cassette recorder, terminal, etc
- Unknown how long Commodore made these after buyout
- Synertek made SYM-1
- Rockwell made AIM-65 with full keyboard & printer


AIM 65
SYM-1
KIM-1
KIM
UNO
Junior
PAL-1
REPRO
DUCTION
KIM
Clone
MICRO
KIM

Programming

- Most people are familiar with programming in various “high level” languages: C, Fortran, BASIC, Pascal, Java, Python, et al.
- These languages are designed to allow people to express their ideas.
- The programs written would be converted to machine code by a compiler or interpreter. How efficient this would be can vary.
- Computers understand machine code.
- Machine code is made of “op codes” in binary
- Assembly language is a way to convert machine op codes to a more human readable format.

Assembly Language

- Assembly language allows us to write human readable code that is directly translated into machine language (plus add comments)
  - Each processor will have a different set of op codes, and thus a different assembly language, but there will be similarities.
- Examples from 6502: [it has 55 commands vs 72 of 6800]
  - ADC Add with carry to A (Accumulator)
  - CMP Compare with A
  - LDA Load Accumulator
  - SBC Subtract with carry to A
  - STR Store A (in a location)
- Assemblers allow for programmer to add comments for use in

More on assembly language

- A “Macro Assembler” adds some elements from higher level languages, such as macros.
- A “cross assembler” runs on one computer, but outputs code for another. Many early computers had their code developed this way.
- A “disassembler” converts machine code into assembly language, tho without the comments.

```
;THIS SUBROUTINE ARRANGES THE 8-BIT ELEMENTS OF A LIST IN ASCENDING
;ORDER.  THE STARTING ADDRESS OF THE LIST IS IN LOCATIONS $30 AND
;$31.  THE LENGTH OF THE LIST IS IN THE FIRST BYTE OF THE LIST.  LOCATION
;$32 IS USED TO HOLD AN EXCHANGE FLAG.

SORT8    LDY #$00       ;TURN EXCHANGE FLAG OFF (= 0)
         STY $32
         LDA ($30),Y    ;FETCH ELEMENT COUNT
         TAX            ; AND PUT IT INTO X
         INY            ;POINT TO FIRST ELEMENT IN LIST
         DEX            ;DECREMENT ELEMENT COUNT
NXTEL    LDA ($30),Y    ;FETCH ELEMENT
         INY
         CMP ($30),Y    ;IS IT LARGER THAN THE NEXT ELEMENT?
         BCC CHKEND
         BEQ CHKEND
                        ;YES. EXCHANGE ELEMENTS IN MEMORY
         PHA            ; BY SAVING LOW BYTE ON STACK.
         LDA ($30),Y    ; THEN GET HIGH BYTE AND
         DEY            ; STORE IT AT LOW ADDRESS
         STA ($30),Y
         PLA            ;PULL LOW BYTE FROM STACK
         INY            ; AND STORE IT AT HIGH ADDRESS
         STA ($30),Y
         LDA #$FF       ;TURN EXCHANGE FLAG ON (= -1)
         STA $32
CHKEND   DEX            ;END OF LIST?
         BNE NXTEL      ;NO. FETCH NEXT ELEMENT
         BIT $32        ;YES. EXCHANGE FLAG STILL OFF?
         BMI SORT8      ;NO. GO THROUGH LIST AGAIN
         RTS            ;YES. LIST IS NOW ORDERED
```

```
void bubble_sort(int arr[], int n) {
 int i, j;
 for (i = 0; i < n - 1; i++) {
  for (j = 0; j < n - i - 1; j++) {
   if (arr[j] > arr[j + 1]) {
    int temp = arr[j];
    arr[j] = arr[j + 1];
    arr[j + 1] = temp;
   }
  }
 }
}
```

Programming the 6502

- https://skilldrick.github.io/easy6502/
- This site is an ebook with a Javascript assembler & assembler

Resources

- Videos
- Websites
- Books
- Hardware & Software

Videos

- 8-Bit Guy: The 6502 CPU Powered a Whole Generation!
  - https://www.youtube.com/watch?v=acUH4IWe2NQ
- LowSpecGamer: The first LowSpec Processor
  - https://www.youtube.com/watch?v=IP2ZBp9O0mk
- LSG: Intel's worst Nightmare
  - https://www.youtube.com/watch?v=P1aqtfXUCEk
- AI's Geek Lab: The Z80 CPU - 1976 to 2024
  - https://www.youtube.com/watch?v=cbMdq8Dsz6Y

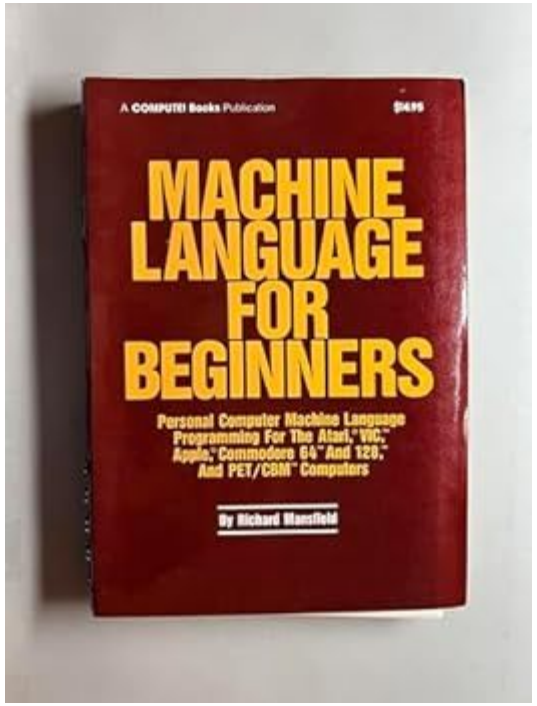
Websites

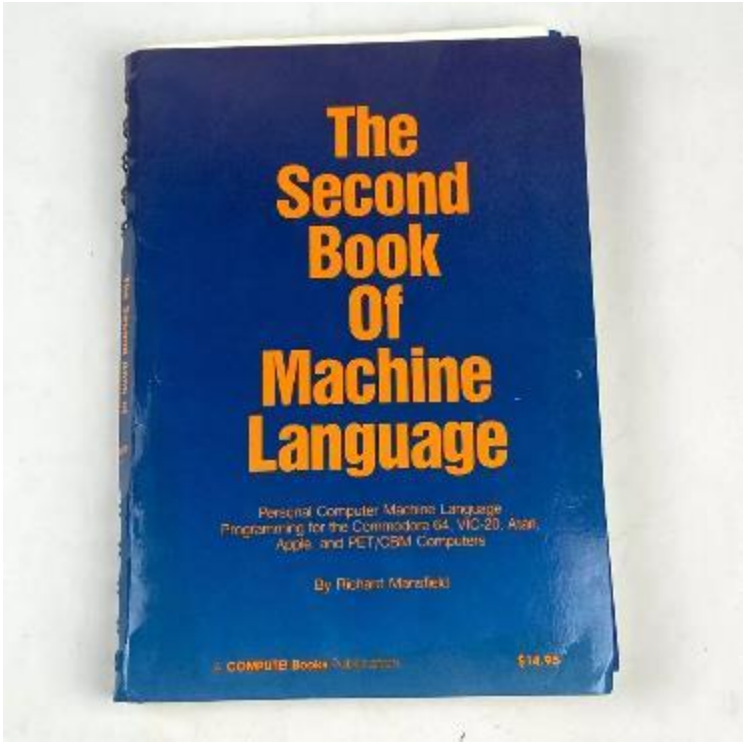
- 6502.org (the 6502 microprocessor resource) http://6502.org/
- RetroComputing: http://retro.hansotten.nl/
  - Pages on 6502, Z80, and KIM-1
- 6502 Primer: https://wilsonminesco.com/6502primer/

Richard Mansfield



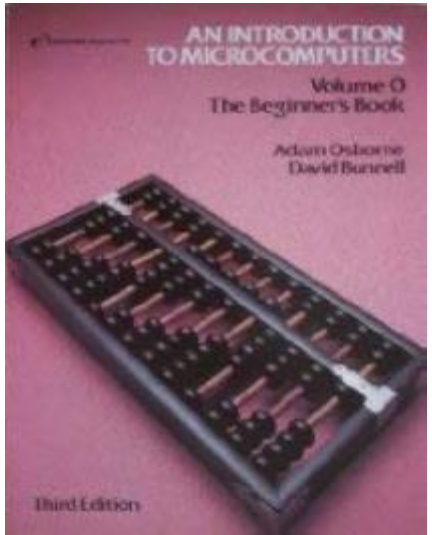
- Published by Compute! Books
- Machine Language for Beginners (1983)
- The Second Book of Machine Language (1984)

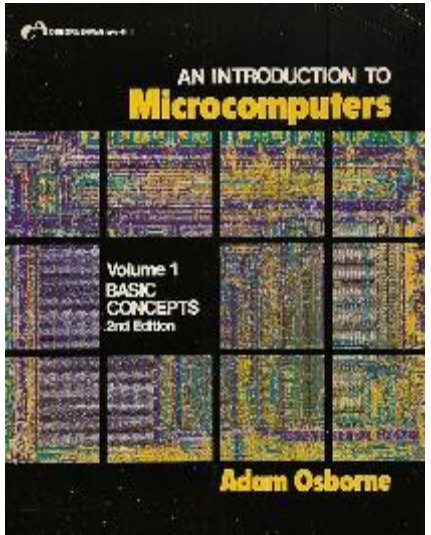


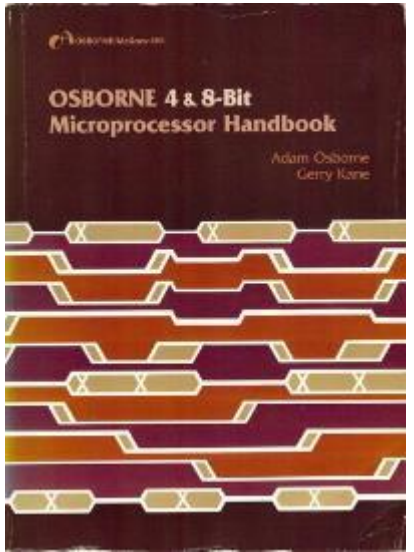


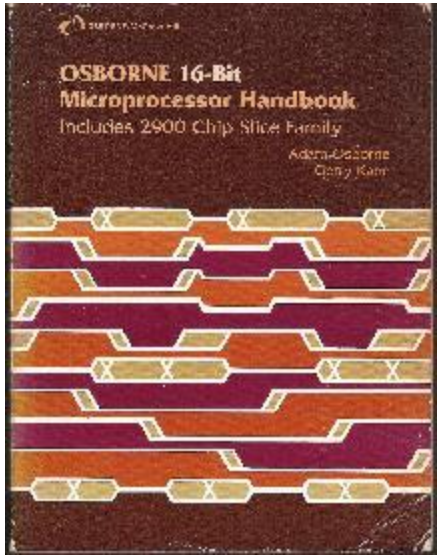
An Introduction to Microcomputers by Osborne

- Volume 0: Beginner's Book, 3rd ed
- Volume 1: Basic Concepts, 2nd ed
- Volume 2: Some Real Products [4-5 editions], replaced by:
  - Osborne 4 & 8-bit Microprocessor Handbook
  - Osborne 16-bit Microprocessor Handbook









MOS Technology booklets for KIM-1

- KIM-1 User Manual
- MOS Programming Manual
- MOS Hardware Manual









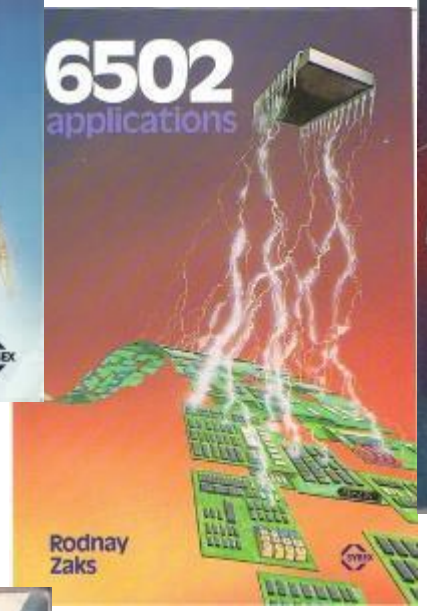
- Available on Tindie

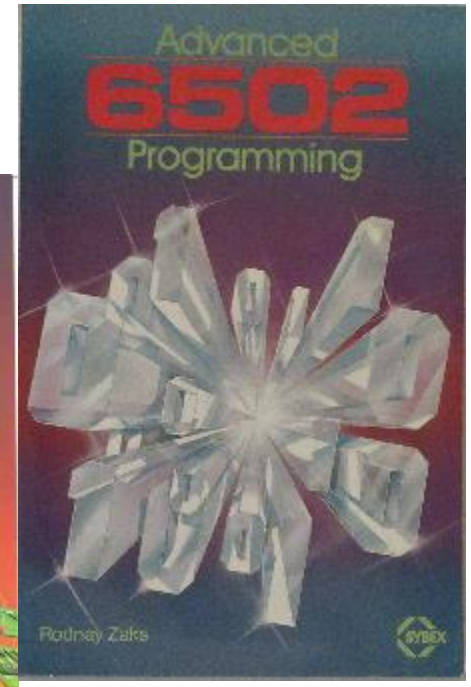
Rodnay Zaks books

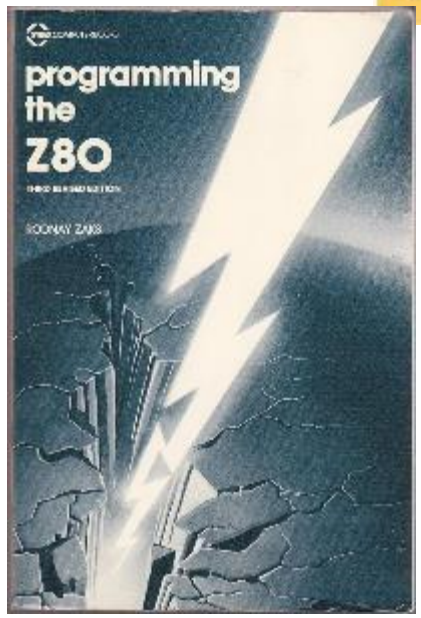
1. Programming the 6502, 4th editi
2. 6502 Applications Book
3. Advanced 6502 Programming
4. 6502 Games

- Also:
  - Programming the Z80, 3rd edition
  - Programming the 6809
  - The CP/M Handbook
  - The Chips to Systems

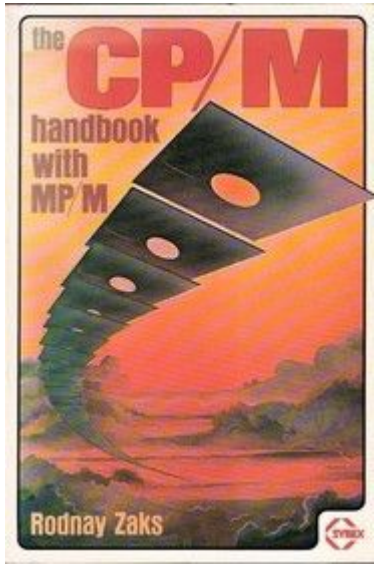










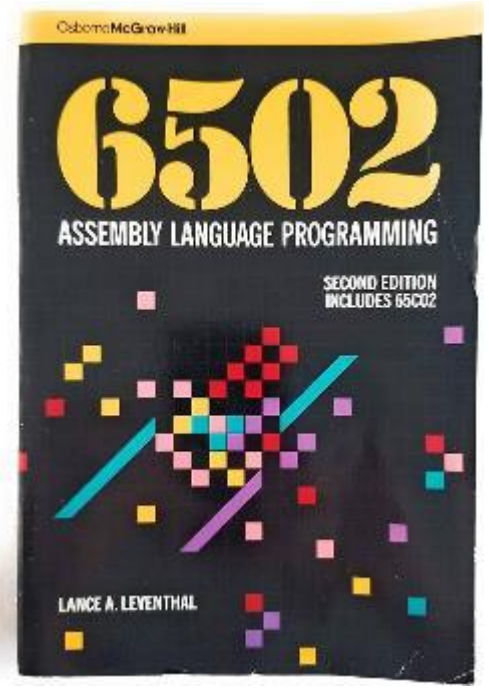


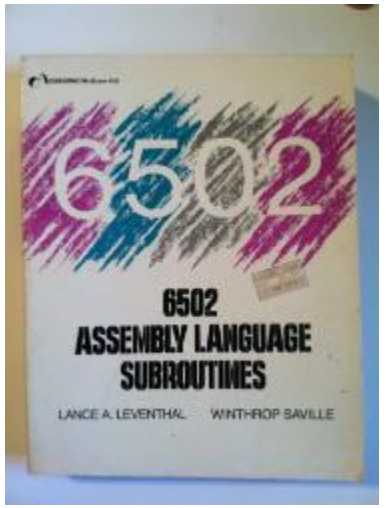
Lance Leventhal books

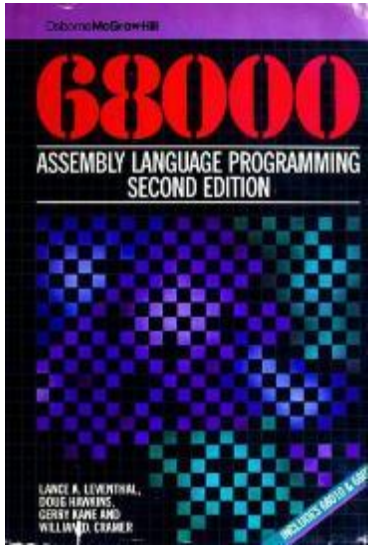
- 6502 Assembly Language Programming, 2nd e
- 6502 Assembly Language Subroutines

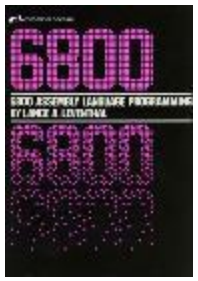
Also

- Z80 Assembly Language Programming
- 6800 Assembly Language Programming
- 6809 Assembly Language Programming
- 68000 Assembly Language Programming, 2nd ed
- & others



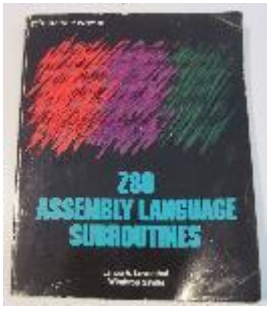






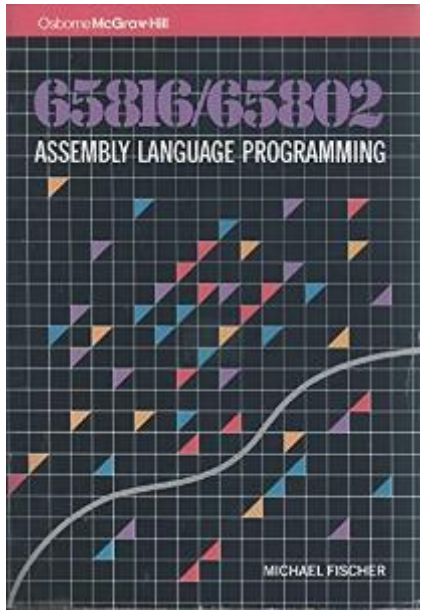


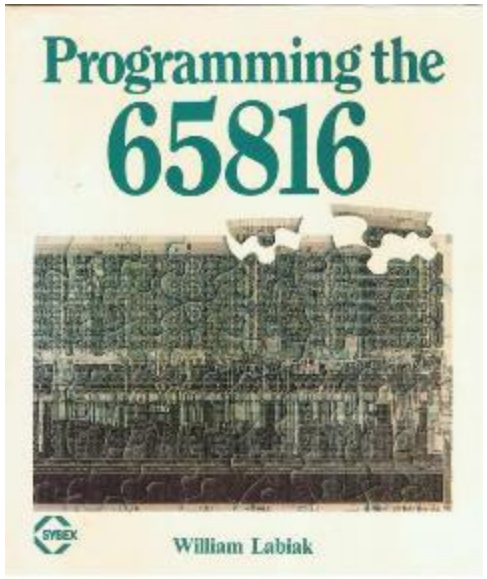




Others

- 65816/65802 Assembly Language Programming
- Programming the 65816
  - Originally from Brady, now reprinted by Western Design







Hardware

- Want to program on a 6502-based systems? Here are some suggestions.

- There are many communities of fans around many classic systems (Apple, Atari, Commodore, Acorn, TI, Sinclair, etc)
- Many in these communities create new hardware for these systems, including replacement boards, new chips via FPGA, etc

Classic 8-bit systems

- Apple II
- Atari 8-bit (400/800/XL/XE)
- Commodore 64/128

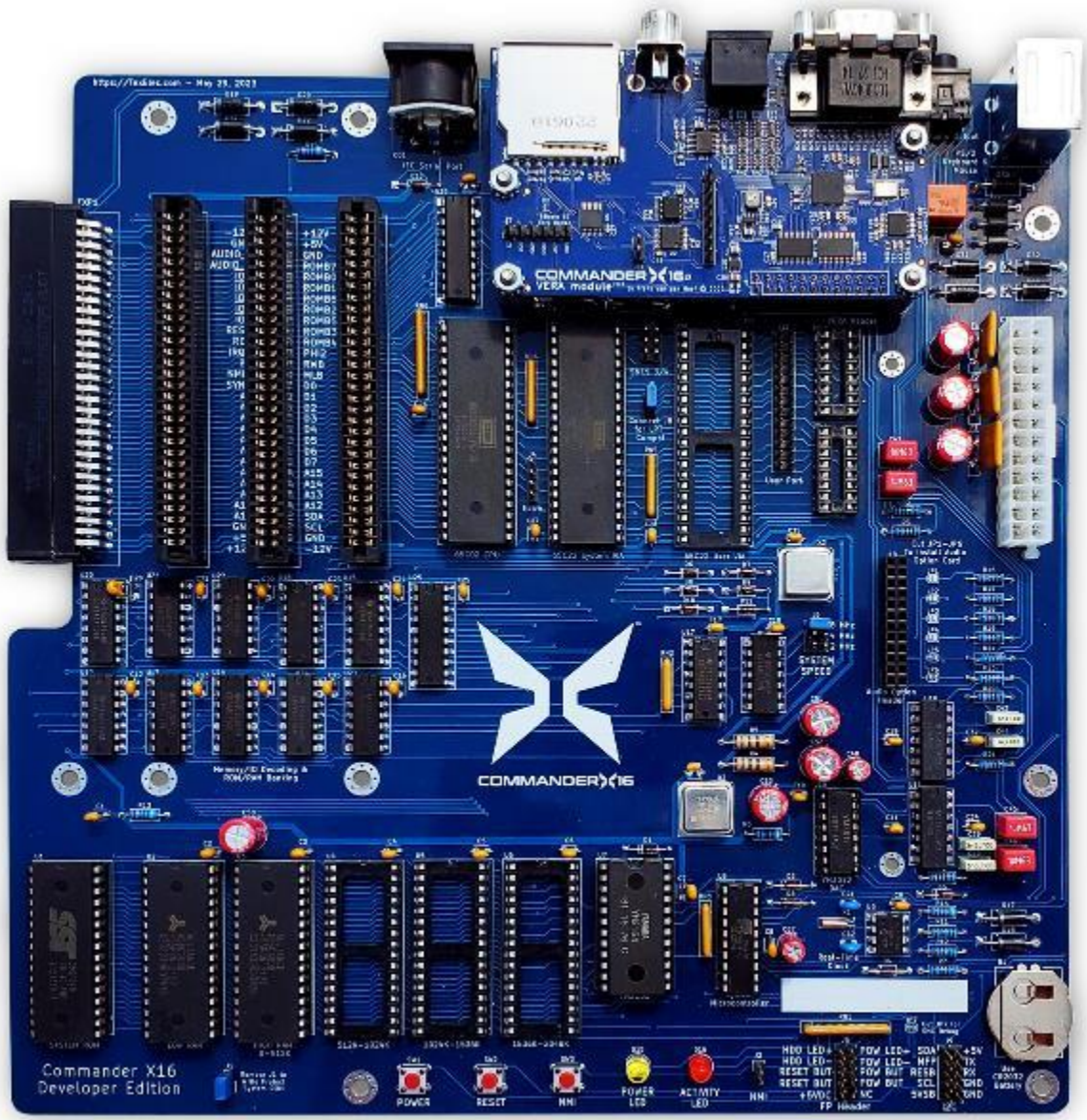






Commander X16

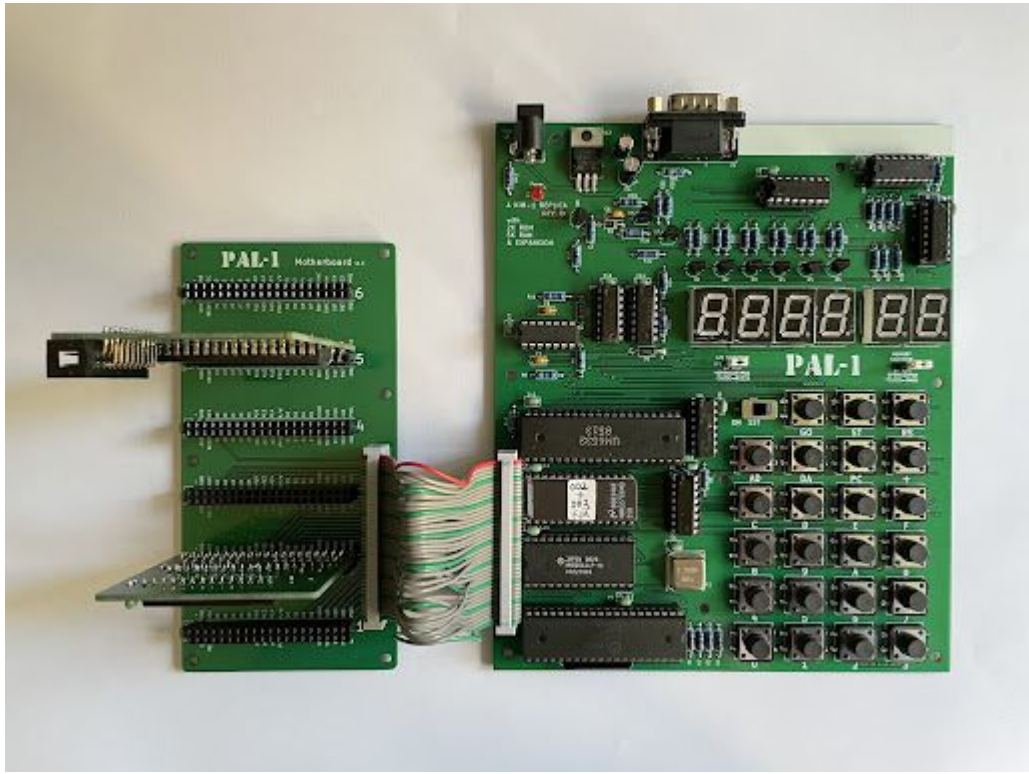
- NEW 6502-based system
- Developer system available
- Specs
  - WDC65C02
  - 512KB RAM, expandable
  - 512KB ROM, expandable
  - Commodore BASIC
  - Yamaha YM2151 Sound chip
  - Graphics
  - Expansion slots
- https://www.commanderx16.com/



KIM-1 clones

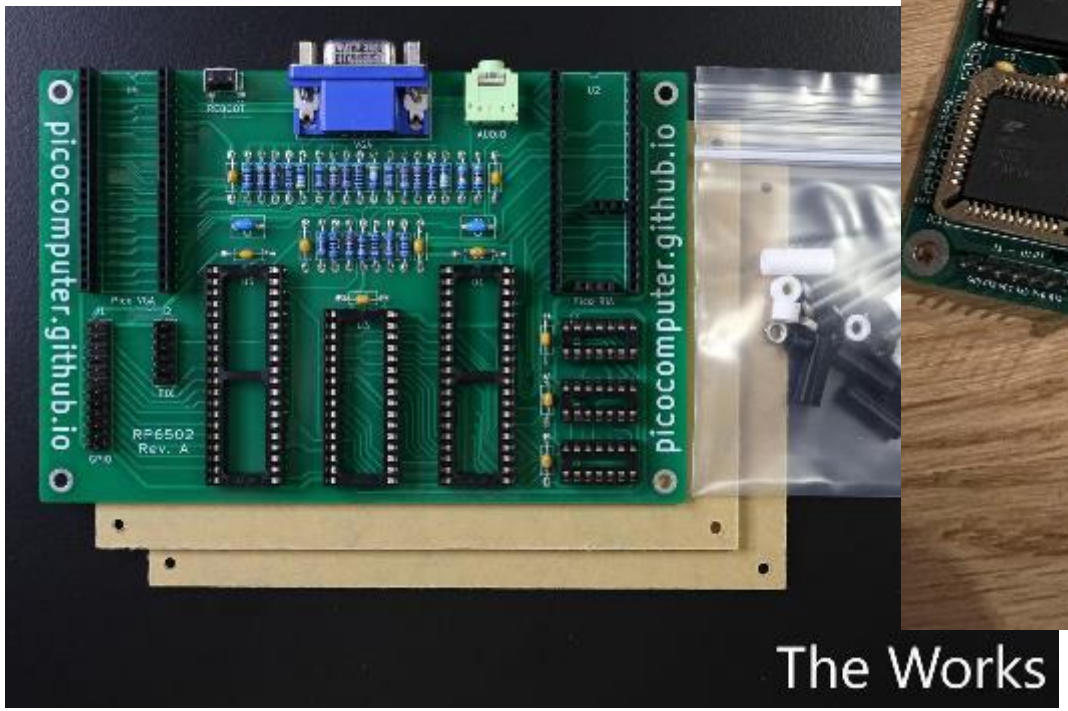
- KIM-1 was the single-board created by MOS to show off the 6502
- Originals are expensive
- BUT there are repros
- PAL-1 i



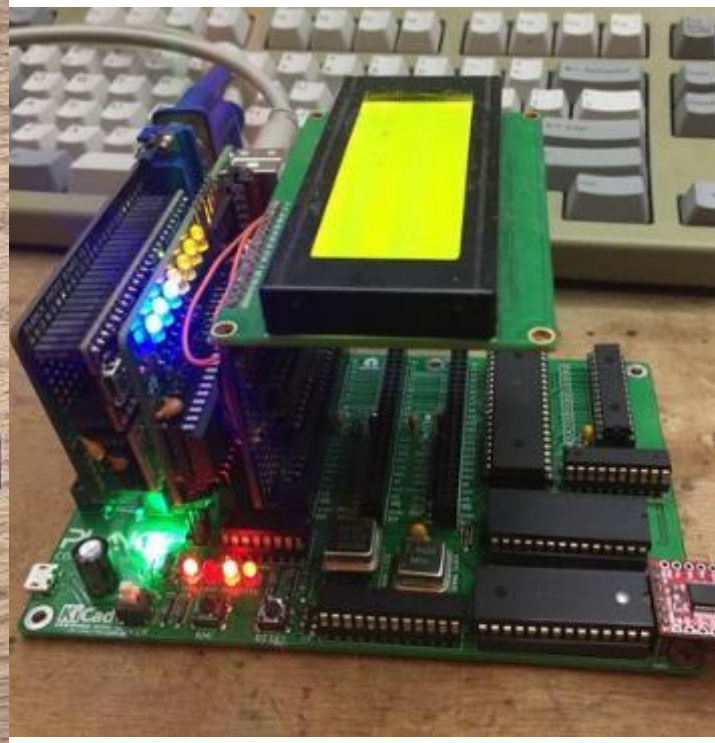


Other 6502-based systems (from Tindie)

- Picocomputer 6502
- Rosco_6502
- Planck 6502 Computer

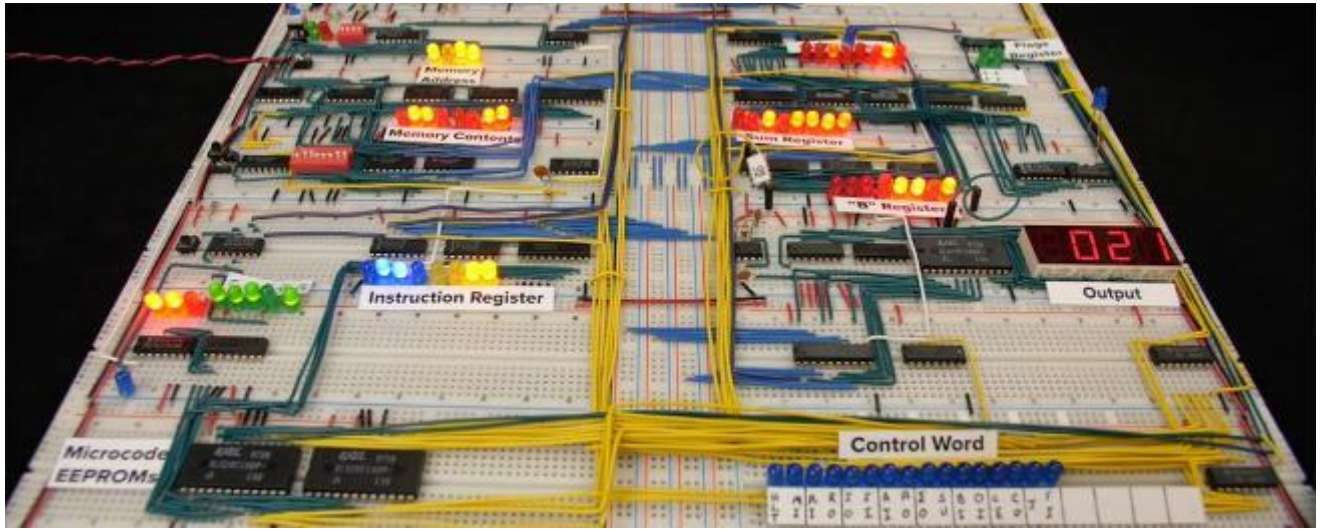






More hardware

- Ben Eater's 6502-based system (breadboard based)
  - https://www.youtube.com/c/beneater
    - https://www.youtube.com/watch?v=HyznrdDSSGM&list=PLowKtXNTBypGqImE405J2565dvjafglHU&index=2
    - https://www.youtube.com/watch?v=LnzuMJLZRdU&list=PLowKtXNTBypFbtuVMUVXNR0z1mu7dp7eH&index=2
  - https://eater.net/



Hardware alternatives

- Emulation using FPGA
- Emulation using Raspberry Pi
  - Ex: PICO-56 (see Tindie)
- Software emulation

QUESTIONS?

EXTRA SLIDES

Intel 8080

- Released in 1974, discontinued in 1990
- 8bit data bus, 16bit address bus (64K)
- 55 instructions (opcode) [vs 77 in 6800]
- 40-pin DIP
- Based on the 8008, itself based on the Datapoint 2200 terminal
- By 1979, cost was $3-4
- Federico Faggin designed, with the help of Masatoshi Shima. They also designed the 4004, 4040, and 8008. And would create the Z80.
- 8080A and 8085 were improved versions.

8080 & Z80

Intel 8080 registers

15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00 *(bit position)*

Main registers

A	Flags	**P**rogram **S**tatus **W**ord
B	C	**B**
D	E	**D**
H	L	**H** (indirect address)

Index registers

SP	**S**tack **P**ointer

Program counter

PC	**P**rogram **C**ounter

Status register

S Z 0 A_C 0 P 1 C	Flags [17]

Zilog Z80 registers

15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00 *(bit position)*

Main registers

Accumulator (A)	Flags (F)	AF
B	C	BC
D	E	DE
H	L	HL

Alternate (shadow) registers

Accumulator' (A')	Flags' (F')	AF'
B'	C'	BC'
D'	E'	DE'
H'	L'	HL'

Index registers

Index X	IX
Index Y	IY
Stack Pointer	SP

Other registers

Interrupt vector	I
Refresh counter	R

Program counter

Program Counter	PC

Status register

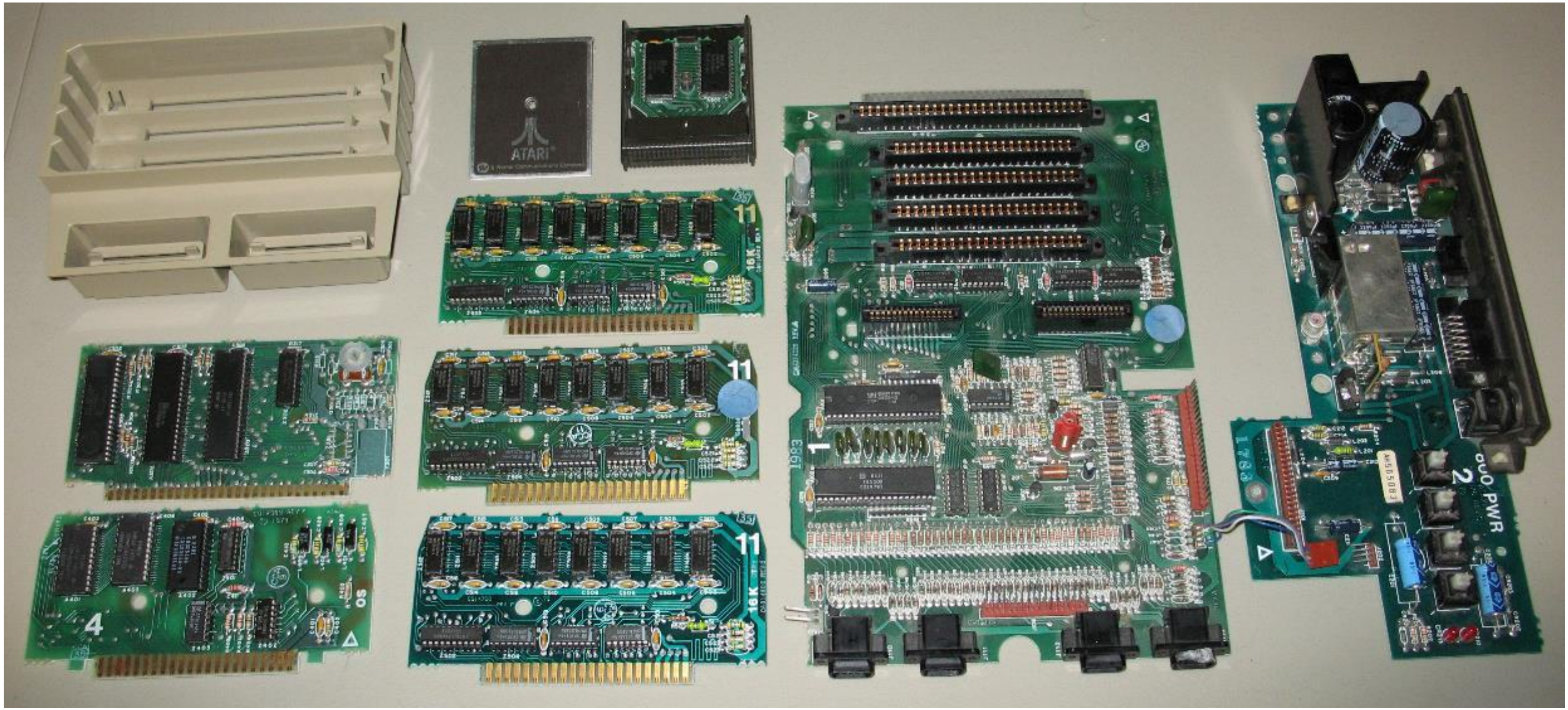
S Z - H - P/V N C	Flags

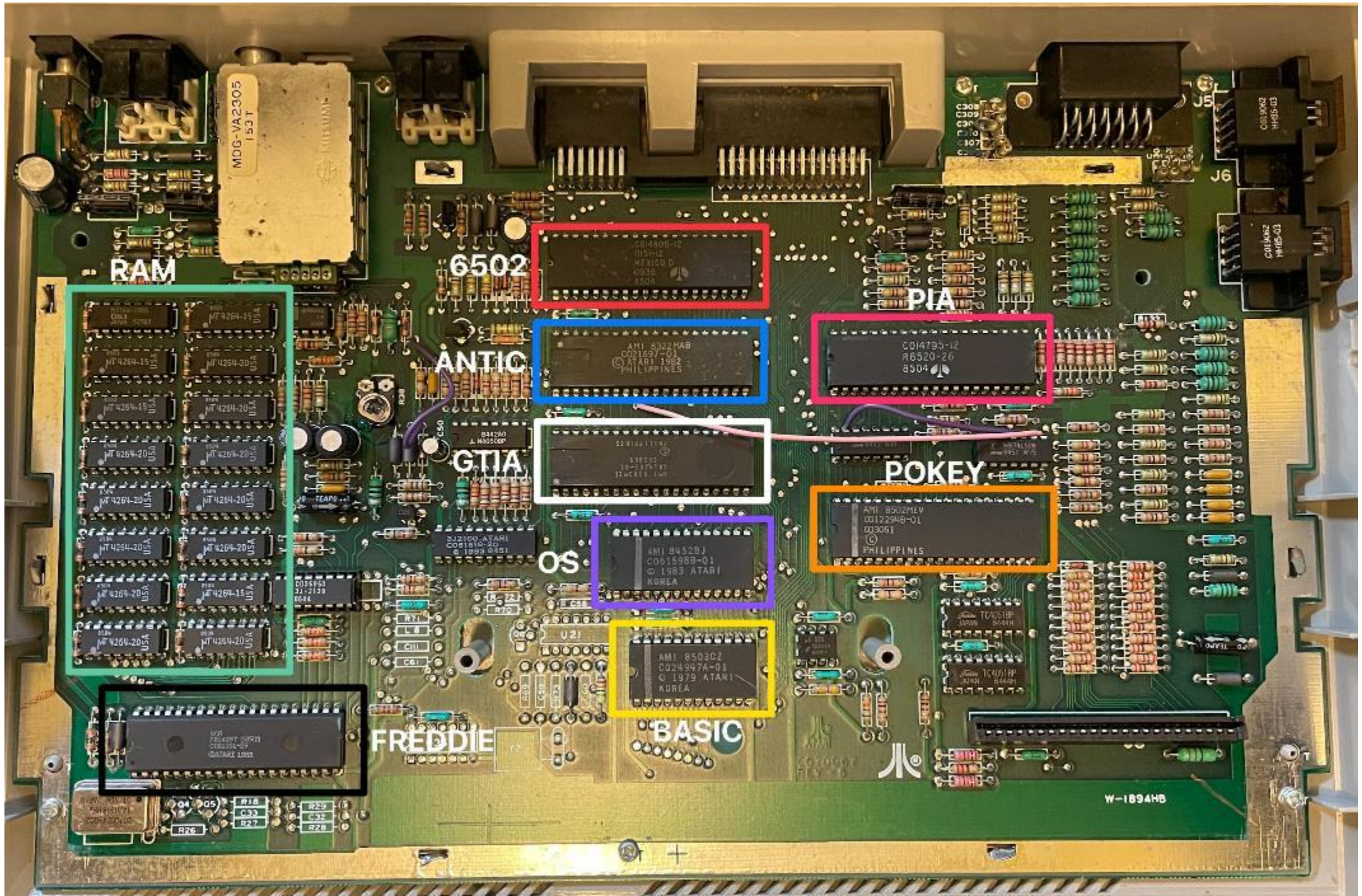
Z80 (and variants) usage

- MANY CP/M-80 based systems
- MANY embedded systems
- MANY systems as a secondary processor (NOT the CPU)
- Osborne-1
- Sinclair ZX Spectrum
- TRS-80 Model I, II, III, IV
- Colecovision
- Nintendo Gameboy
- Sega Master system
- TI-8x graphing calculators

Atari 8-bit

- 6502- originally 6502B, later “SALLY” (aka “6502C”)
- ANTIC [Alphanumeric Television Interface Controller]
  - GPU coprocessor
- CTIA/GTIA [Color/Graphics Television Interface Adaptor
  - Graphics controller
- POKEY [Pot Keyboard Integrated Circuit]
  - Sound, serial, keyboard, paddles
- PIA [6520, Peripheral Interface Adapter]
  - Joysticks, etc
- FREDDIE
  - Memory decoder & timer, added to XE line. EMMU does bank-switching


ATARI
11
16K
11
11
16K
4
OS
1
1983
2
PWR


RAM
6502
PIA
ANTIC
GTIA
POKEY
OS
FREDDIE
BASIC