

GLADIC IP BRIEF

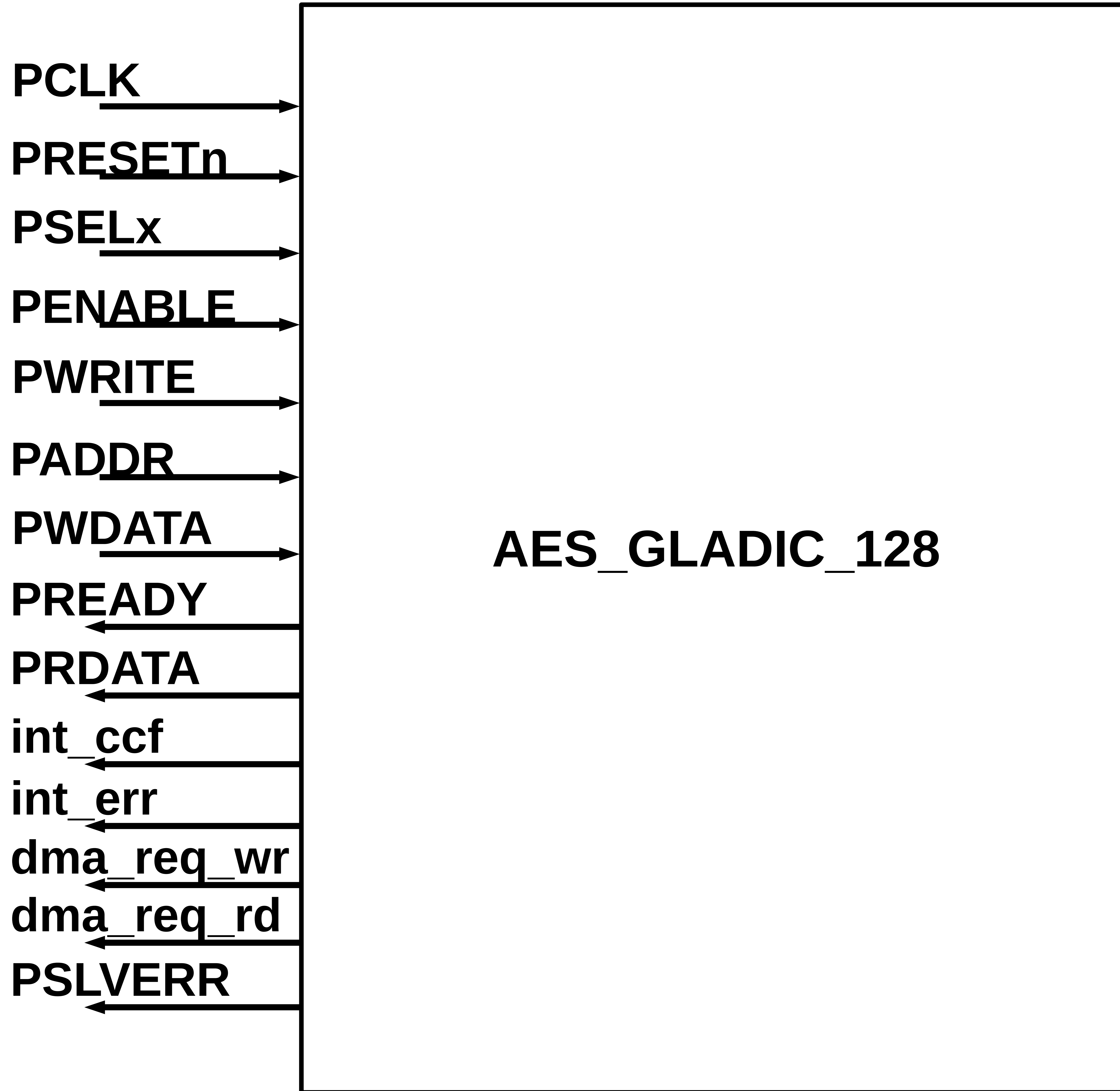
Name : Felipe Fernandes da Costa
Júlio Cesar Soares Américo Filho

Linkedin: br.linkedin.com/pub/felipe-fernandes/35/a9b/87b

SUMMARY

- **TOP BLOCK DIAGRAM**
- **TOP BLOCK PIN DESCRIPTION**
- **INTERNAL REGISTER DESCRIPTION**
- **ENVIRONMENT DIAGRAM**
- **MACHINE STATE BFMs**
- **ECB STRUCT WRITE / READ DATATYPE**
- **CBC STRUCT WRITE / READ DATATYPE**
- **CTR STRUCT WRITE / READ DATATYPE**
- **USEFUL LINKS**

TOP BLOCK DIAGRAM



TOP BLOCK PIN DESCRIPTION

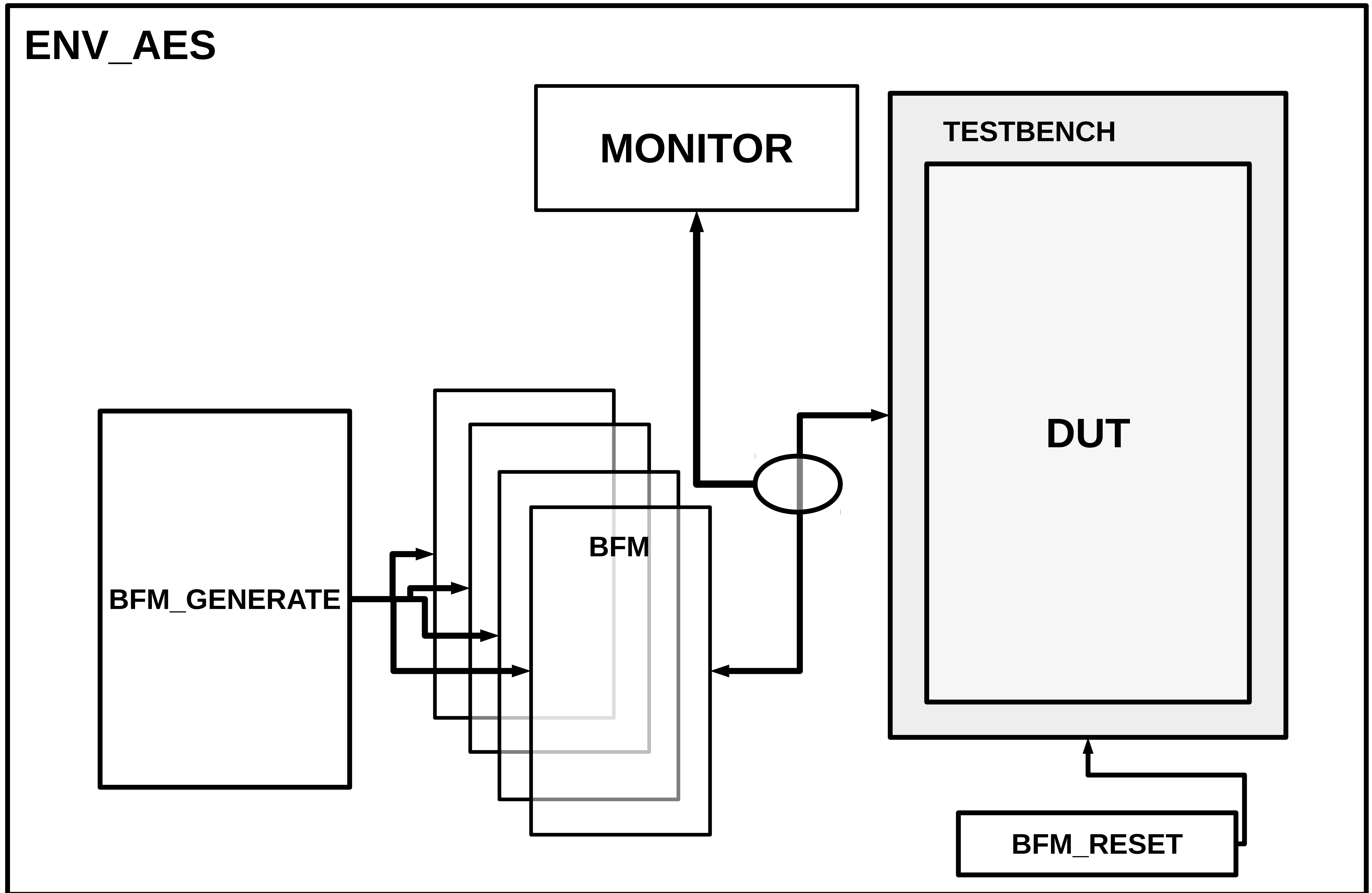
PIN DESCRIPTION			
PIN NAME	DIRECTION	SIZE	DESCRIPTION
PCLK	INPUT	1	Posedge Clock
PRESETn	INPUT	1	Reset negate
PSELx	INPUT	1	Enable Core
PENABLE	INPUT	1	Response from core APB to valid data
PWRITE	INPUT	1	1'b1 to Write and 1'b0 to Read
PADDR	INPUT	32	Address according ARM processor spec
PWDATA	INPUT	32	Used to write data on Core
PREADY	OUTPUT	1	This indicate to valid data and always on 1'b1
PRDATA	OUTPUT	32	Read data from core
int_ccf	OUTPUT	1	Interruption flag aes core finished
int_err	OUTPUT	1	Interruption flag aes error
dma_req_wr	OUTPUT	1	DMA request to write data on core
dma_req_rd	OUTPUT	1	DMA request to read data from core
PSLVERR	OUTPUT	1	Used to indicate error. This is not used.

INTERNAL REGISTER DESCRIPTION

CORE ADDRESS REGISTER INFO			
NAME	ADDR	SIZE*	DESCRIPTION
AES_CR	0x00h	12	CONFIGURATION REGISTER
AES_SR	0x04h	3	STATUS REGISTER
AES_DINR	0x08h	32	DATA INPUT REGISTER
AES_DOUTR	0x0Ch	32	DATA OUTPUT REGISTER
AES_KEYR0	0x10h	32	KEY REGISTER LSW
AES_KEYR1	0x14h	32	KEY REGISTER
AES_KEYR2	0x18h	32	KEY REGISTER
AES_KEYR3	0x1Ch	32	KEY REGISTER MSW
AES_IVR0	0x20h	32	INITIALIZATION VECTOR REGISTER LSW
AES_IVR1	0x24h	32	INITIALIZATION VECTOR REGISTER
AES_IVR2	0x28h	32	INITIALIZATION VECTOR REGISTER
AES_IVR3	0x2Ch	32	INITIALIZATION VECTOR REGISTER MSW

* Some registers doesnt use all 32 bit register.

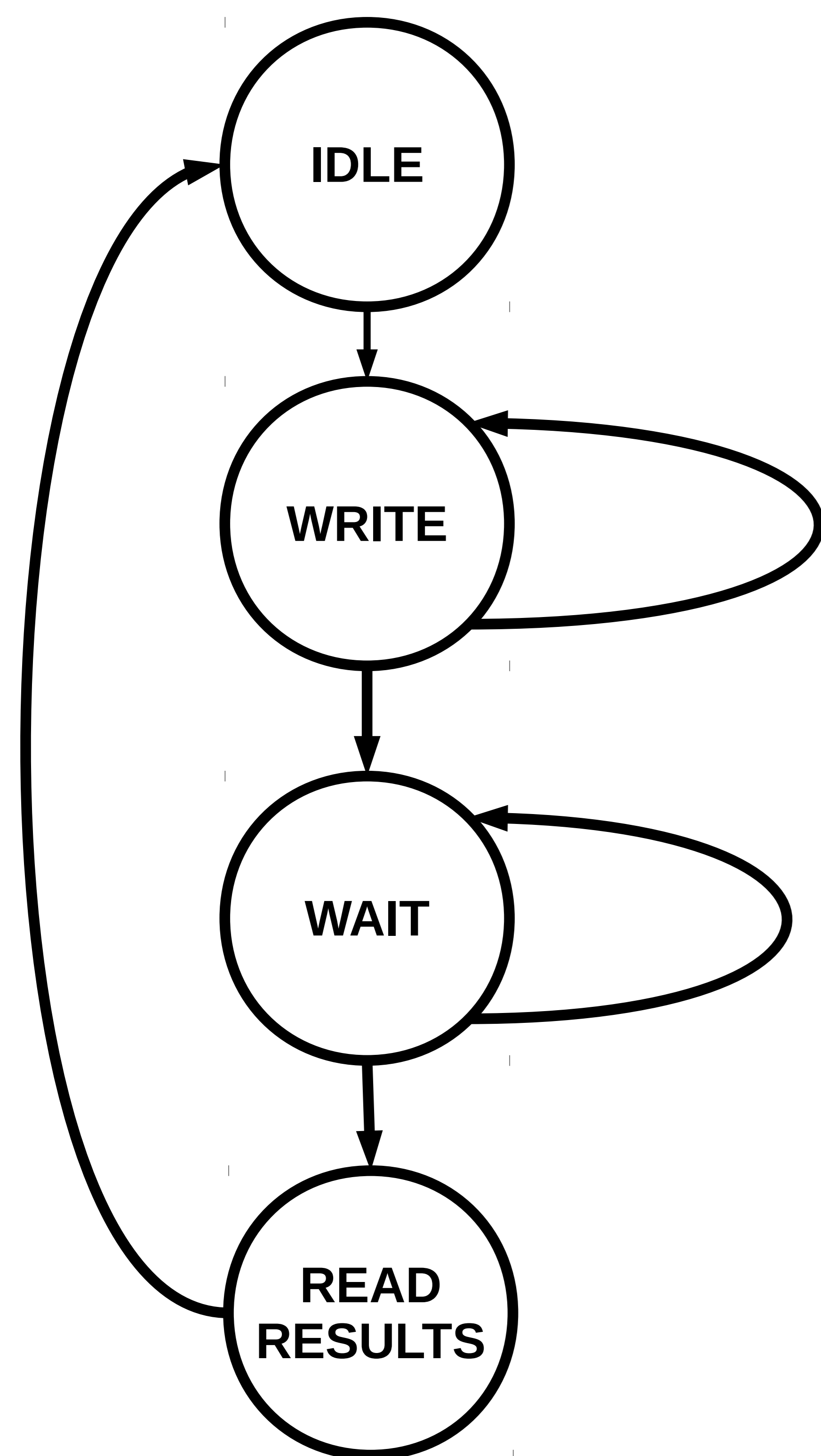
ENVIRONMENT DIAGRAM



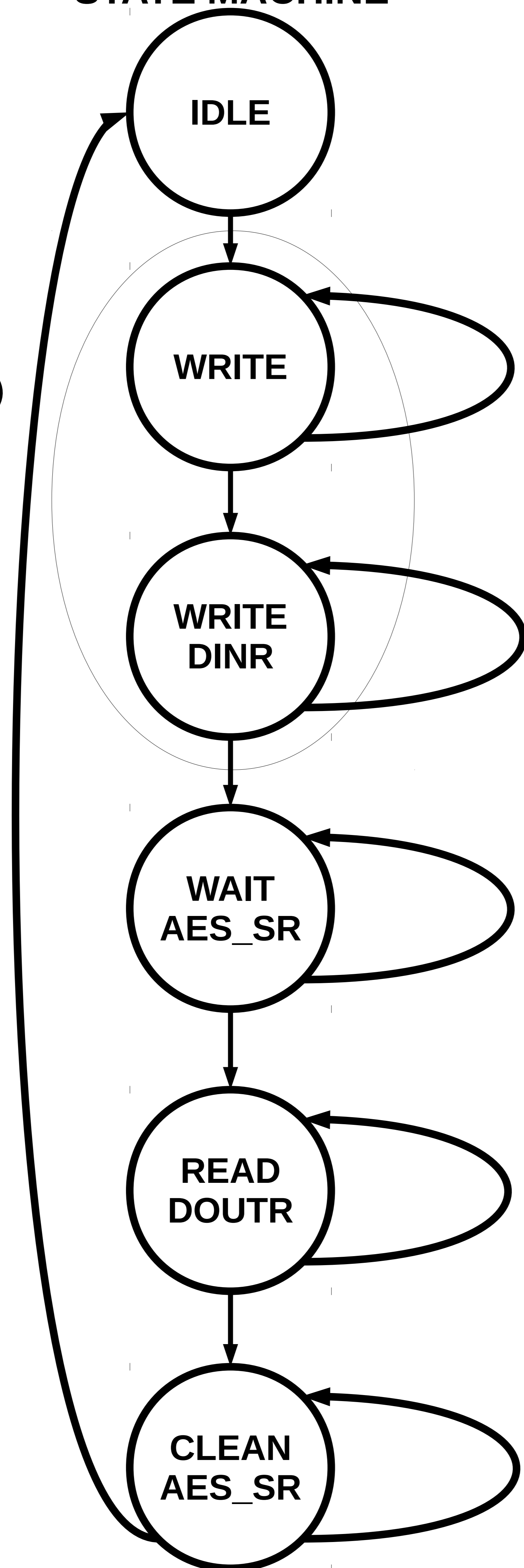
MACHINE STATES BFMs

* State machine examples

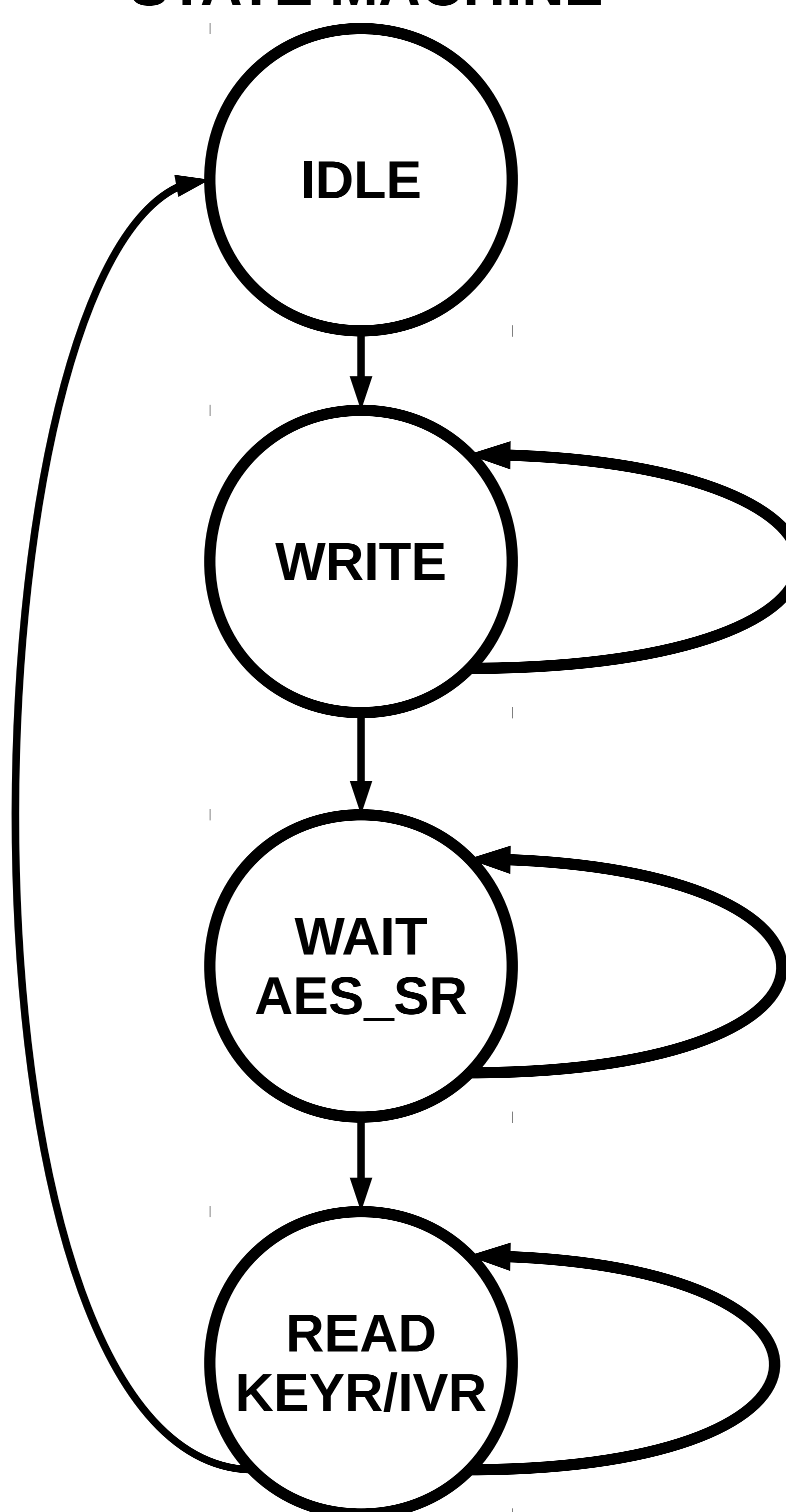
WRITE – READ
STATE MACHINE



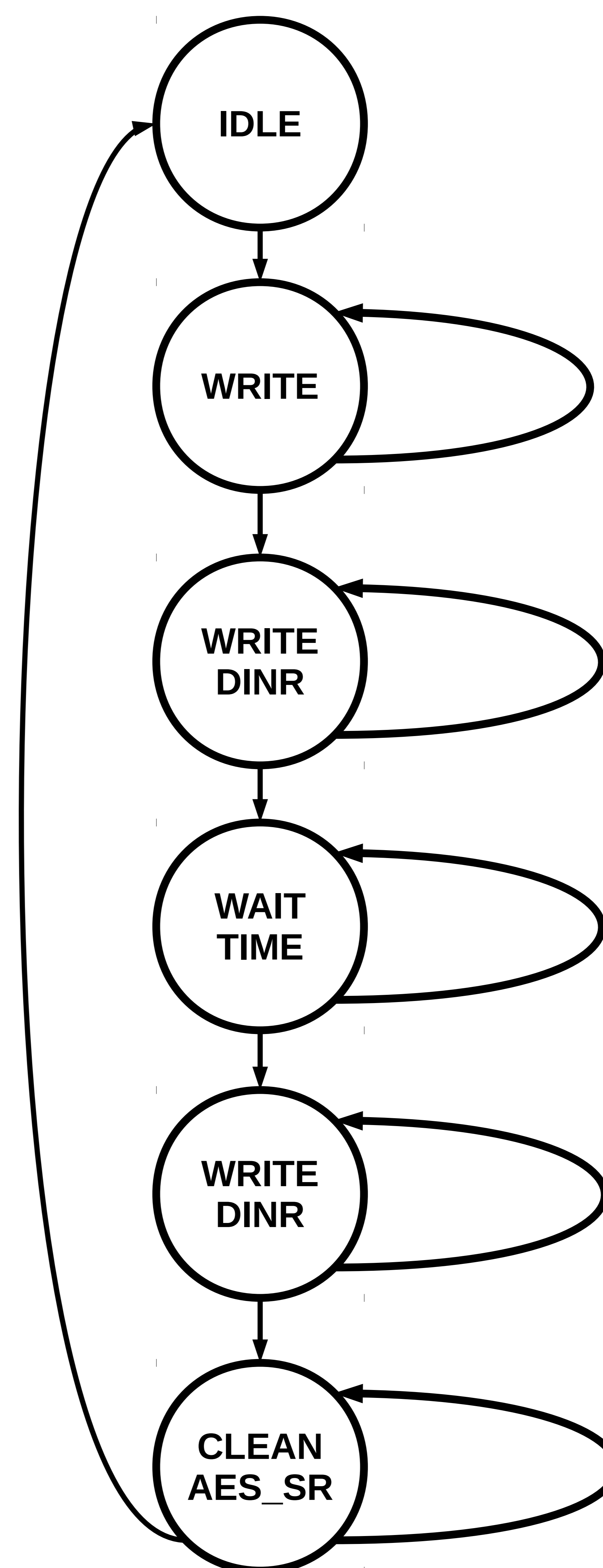
WRITE – READ
DOUTR ONLY
STATE MACHINE



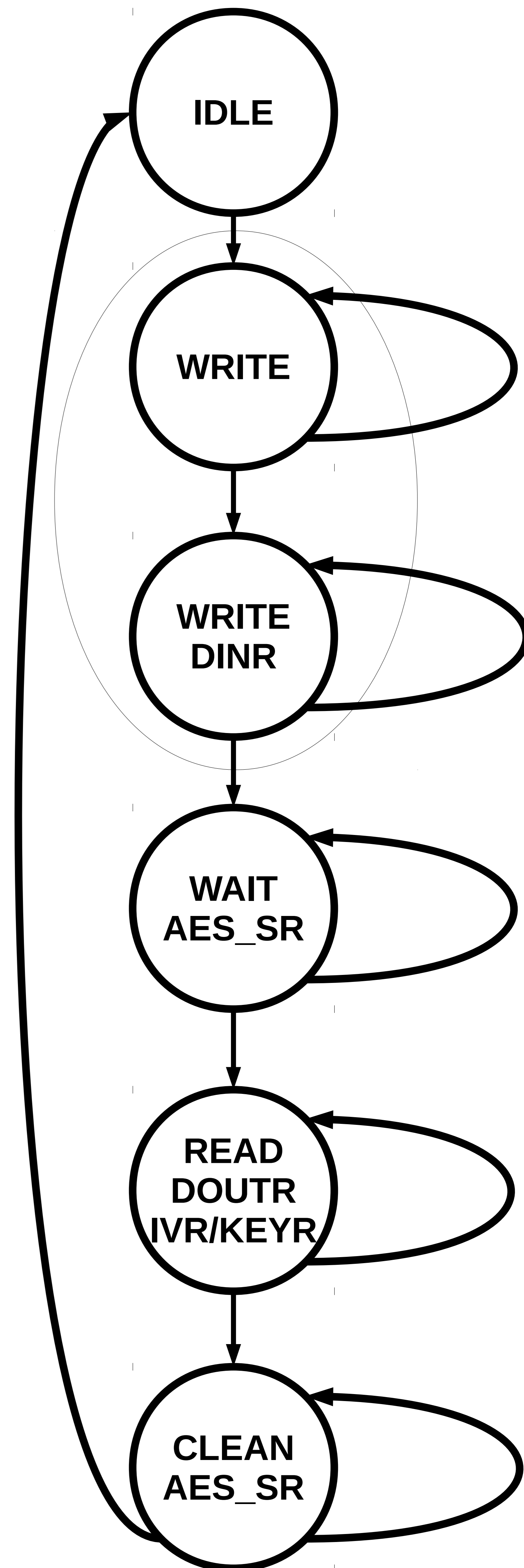
WRITE – READ
KEYR/IVR ONLY
STATE MACHINE



WRITE DINR ONLY
STATE MACHINE



WRITE – READ
DINR/KEYR/IVR
STATE MACHINE



ECB ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_00

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

00112233

44556677

8899AABB

CCDDEEFF

KEYRX

00010203

04050607

08090A0B

0C0D0E0F

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

69C4E0D8

6A7B0430

D8CDB780

70B4C55A

DKEY

13111D7F

E3944A17

F307A78B

4D2B30C5

ECB ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_01

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

22330011

66774455

AABB8899

EEFFCCDD

KEYRX

00010203

04050607

08090A0B

0C0D0E0F

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

E0D869C4

04306A7B

B780D8CD

C55A70B4

DKEY

13111D7F

E3944A17

F307A78B

4D2B30C5

ECB ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_02

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

22330011

66774455

AABB8899

EEFFCCDD

KEYRX

00010203

04050607

08090A0B

0C0D0E0F

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

15DA8D52

2777A369

6D2C495B

0813BF90

DKEY

13111D7F

E3944A17

F307A78B

4D2B30C5

ECB ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_03

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

22330011

66774455

AABB8899

EEFFCCDD

KEYRX

00010203

04050607

08090A0B

0C0D0E0F

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

A3B412DA

43047B7C

21EC500A

DF0BF677

DKEY

13111D7F

E3944A17

F307A78B

4D2B30C5

CBC ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_00

DINR3	DINR2	DINR1	DINR0
IVR3	IVR2	IVR1	IVR0
KEYR3	KEYR2	KEYR1	KEYR0

MSW

LSW

TEXTX	6BC1BEE2	2E409F96	E93D7E11	7393172A
KEYRX*	2B7E1516	28AED2A6	ABF71588	09CF4F3C
IVRX	00010203	04050607	08090A0B	0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT	7649ABAC	8119B246	CEE98E9B	12E919D7
DKEY	D014F9A8	E3944A17	F307A78B	4D2B30C5

*On decryption mode you must do decryption with key generated

CBC ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_01

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX*

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

ABAC7649

B2468119

8E9BCEE9

19D712E9

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

*On decryption mode you must do decryption with key generated

CBC ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_03

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX*

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

70195AF6

92A82859

D079A272

30AF0AC4

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

*On decryption mode you must do decryption with key generated

CBC ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_02

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX*

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

00010203

04050607

08090A0B

0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT

CD2994FC

F6AE2796

7DA445FA

289EE839

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

*On decryption mode you must do decryption with key generated

CBC ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_03

DINR3	DINR2	DINR1	DINR0
IVR3	IVR2	IVR1	IVR0
KEYR3	KEYR2	KEYR1	KEYR0

MSW

LSW

TEXTX	BEE26BC1	9F962E40	7E11E93D	172A7393
KEYRX*	2B7E1516	28AED2A6	ABF71588	09CF4F3C
IVRX	00010203	04050607	08090A0B	0C0D0E0F

RESULTS : DOUTR/KEY

CTEXT	70195AF6	92A82859	D079A272	30AF0AC4
DKEY	D014F9A8	E3944A17	F307A78B	4D2B30C5

*On decryption mode you must do decryption with key generated

CTR ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_00

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

6BC1BEE2

2E409F96

E93D7E11

7393172A

KEYRX

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

F0F1F2F3

F4F5F6F7

F8F9FAFB

FCFDFFEF

RESULTS : DOUTR/KEY

CTEXT

874D6191

B620E326

1BEF6864

990DB6CE

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

CTR ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_01

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

F0F1F2F3

F4F5F6F7

F8F9FAFB

FCFDFFEF

RESULTS : DOUTR/KEY

CTEXT

6191874D

E326B620

68641BEF

B6CE990D

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

CTR ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_02

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

F0F1F2F3

F4F5F6F7

F8F9FAFB

FCFDFFEF

RESULTS : DOUTR/KEY

CTEXT

CD3DE72D

2FEA4ED8

0B073BCF

F38BED79

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

CTR ENCRYPTION / DECRYPTION / DERIVATION DECRYPTION /KEY GENERATION DATATYPE_03

DINR3

DINR2

DINR1

DINR0

IVR3

IVR2

IVR1

IVR0

KEYR3

KEYR2

KEYR1

KEYR0

MSW

LSW

TEXTX

BEE26BC1

9F962E40

7E11E93D

172A7393

KEYRX

2B7E1516

28AED2A6

ABF71588

09CF4F3C

IVRX

F0F1F2F3

F4F5F6F7

F8F9FAFB

FCFDFFEF

RESULTS : DOUTR/KEY

CTEXT

70195AF6

92A82859

D079A272

30AF0AC4

DKEY

D014F9A8

E3944A17

F307A78B

4D2B30C5

USEFUL LINKS

- **ADVANCED ENCRYPTION STANDARD (AES)**
- **Recommendation for BlockCipher Modes of Operation**
- **OPENSSL**