

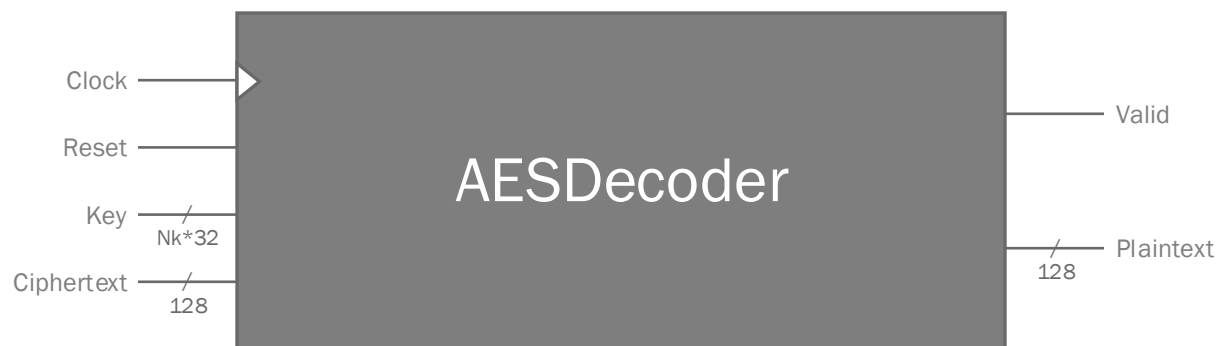
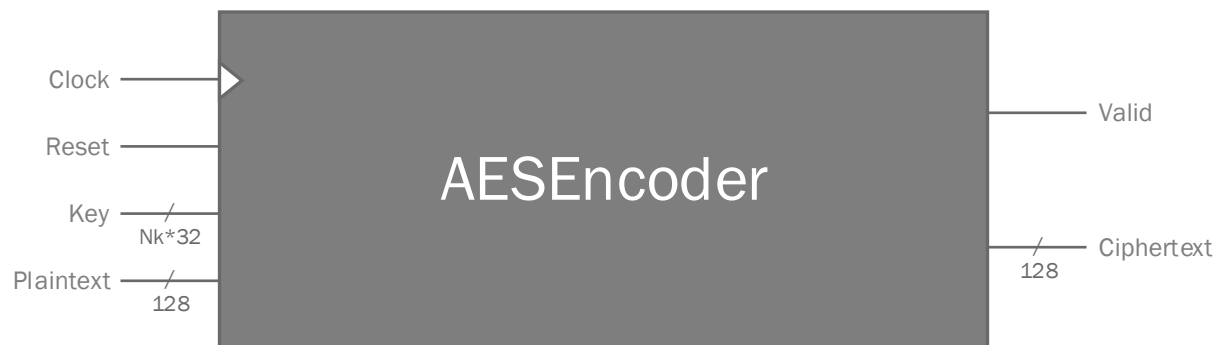
AES Cipher/Inverse Cipher Block Diagram

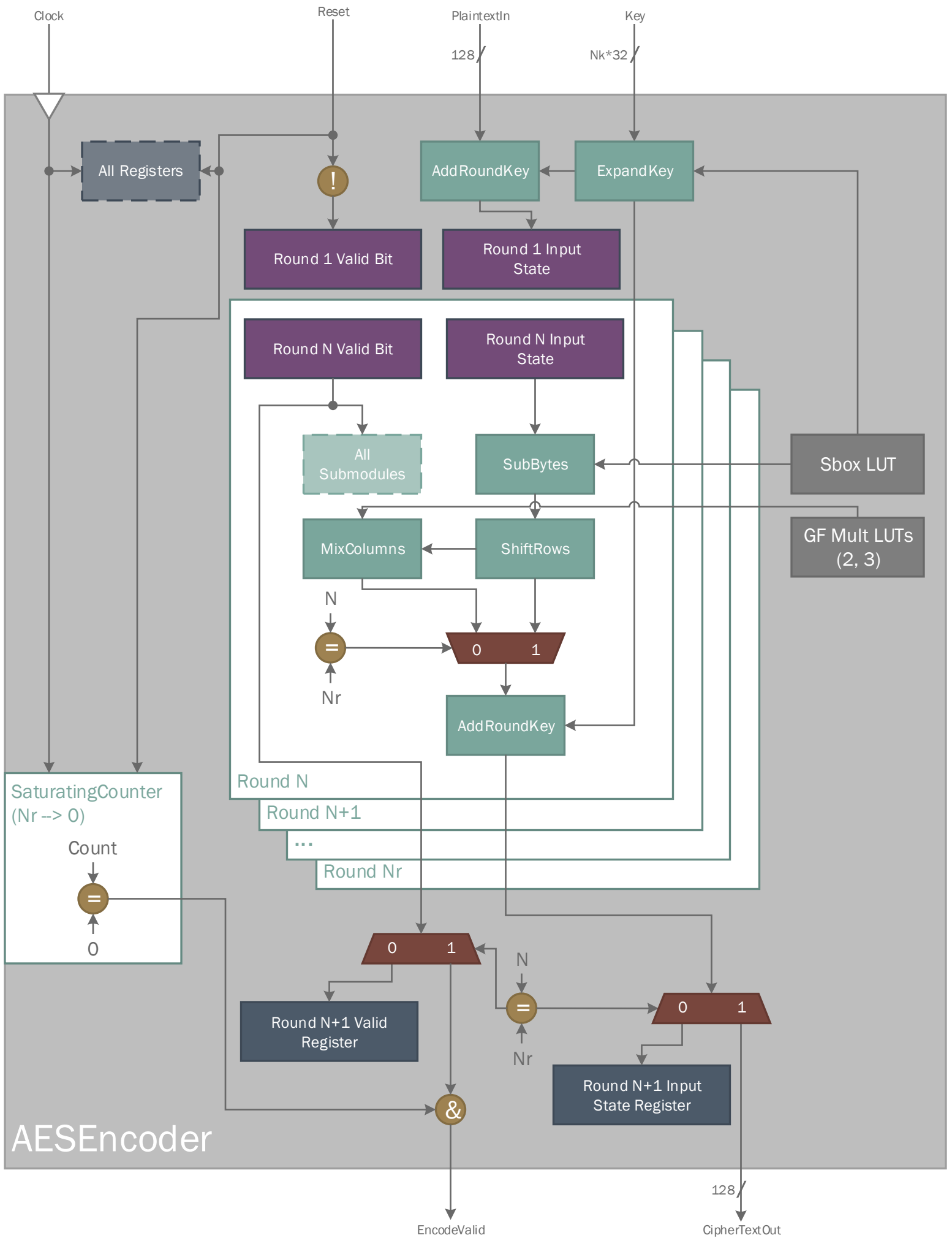
Alex Pearson ECE 571 Final Project
Daniel Collins SP2016
Scott Lawson

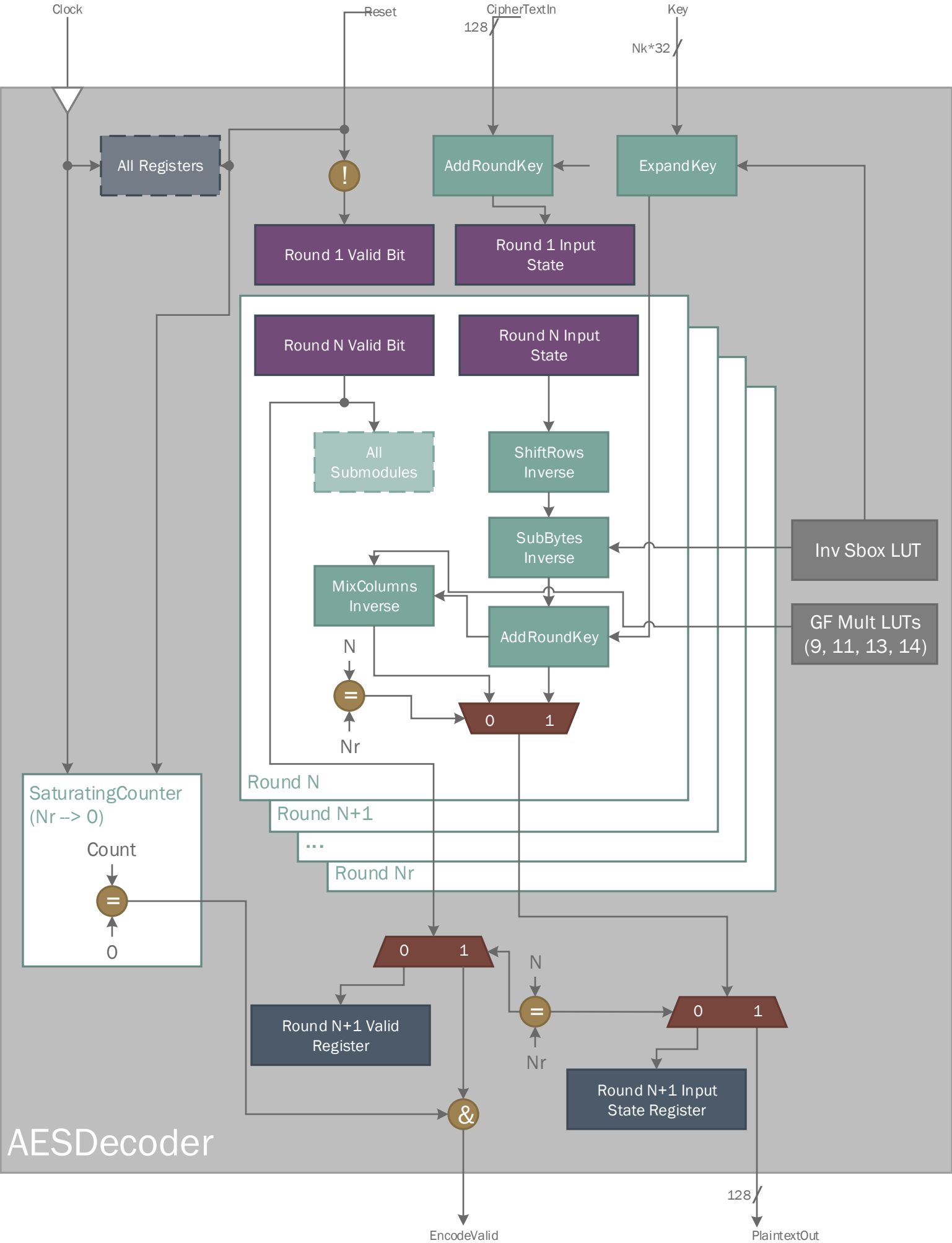
Derived from the AES Standard, Nov 26 2001, issued by NIST
Available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Key:

- Nb Number of 32-bit words comprising the State, input, and output widths
 This value always 4 according to the current version of the standard, so these vectors are
 always 128 bits wide
- Nk Number of 32-bit words comprising the Cipher Key
 Allowed values are 4, 6, or 8 (128-, 196-, and 256-bit wide keys, respectively)
- Nr Number of rounds
 Is 10 when $Nk=4$, 12 when $Nk=6$, and 14 when $Nk=8$







HVL Test Bench

Test Vector Files

Packet =
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }

If Error packet received

Stop on error

{ ERROR, sva }
= Packet

SCEMI INPUT PIPE

SCEMI OUTPUT PIPE

{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
= Packet

Vector
Permutator

PlainText128

Key[0:127]

AESEncoder128

EncodeResult128

CipherText128

Key[0:127]

AESDecoder128

DecodeResult128

PlainText128

Key[0:191]

AESEncoder192

EncodeResult192

CipherText192

Key[0:191]

AESDecoder192

DecodeResult192

PlainText128

Key[0:255]

AESEncoder256

EncodeResult256

CipherText256

Key[0:255]

AESDecoder256

DecodeResult256

Output Integrity
Check
(SVA on Veloce)

PlainText CipherText128 CipherText192 CipherText256

Packet =
{ ERROR, sva }

Transactor (Directed Test)

HVL Test Bench

Test Vector Files

Packet =
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }

If Error packet received

Stop on error

{ ERROR, sva }
= Packet

SCEMI INPUT PIPE

SCEMI OUTPUT PIPE

{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
= Packet

Vector
Permutator

PlainText128

Key[0:127]

AESEncoder128

AESDecoder128

DecodeResult128

PlainText128

Key[0:191]

AESEncoder192

AESDecoder192

DecodeResult192

PlainText128

Key[0:255]

AESEncoder256

AESDecoder256

DecodeResult256

PlainText

Packet =
{ ERROR, sva }

Output Integrity
Check
(SVA on Veloce)

Transactor (Seeded Test)