Tape Logical Block Protection
(aka Tape Checksum)

Kevin D. Butt

SCSI Architect, Data Protection & Retention, IBM

T10/SSC Working Group Secretary

MS 6TYA, 9000 S. Rita Rd., Tucson, AZ 85744

Tel: 520-799-5280

Fax: 520-799-2723 (T/L:321)

**Email address: kdbutt@us.ibm.com**

Traditional methods used to try to get data protection

- **Drive adds protection information to each logical block**
  - vendor-specific format
    - Add CRC
    - Add ECC & other data validation/reconstruction methods
  - after received at drive during process of storing on media

    (next slide shows an animated example)

- **Drive reads after write and validates CRC**
- **Some applications add unique protection information as part of the data**
  - Allows verification that nothing changed, but only when data is read
  - Does not provide detection on write
  - Does not allow for checking at various points during the transfer
  - No method for the drive to validate the blocks without transferring them to the application.
  - Sometimes saves to a database of meta-data

Traditional Protection of Tape Data
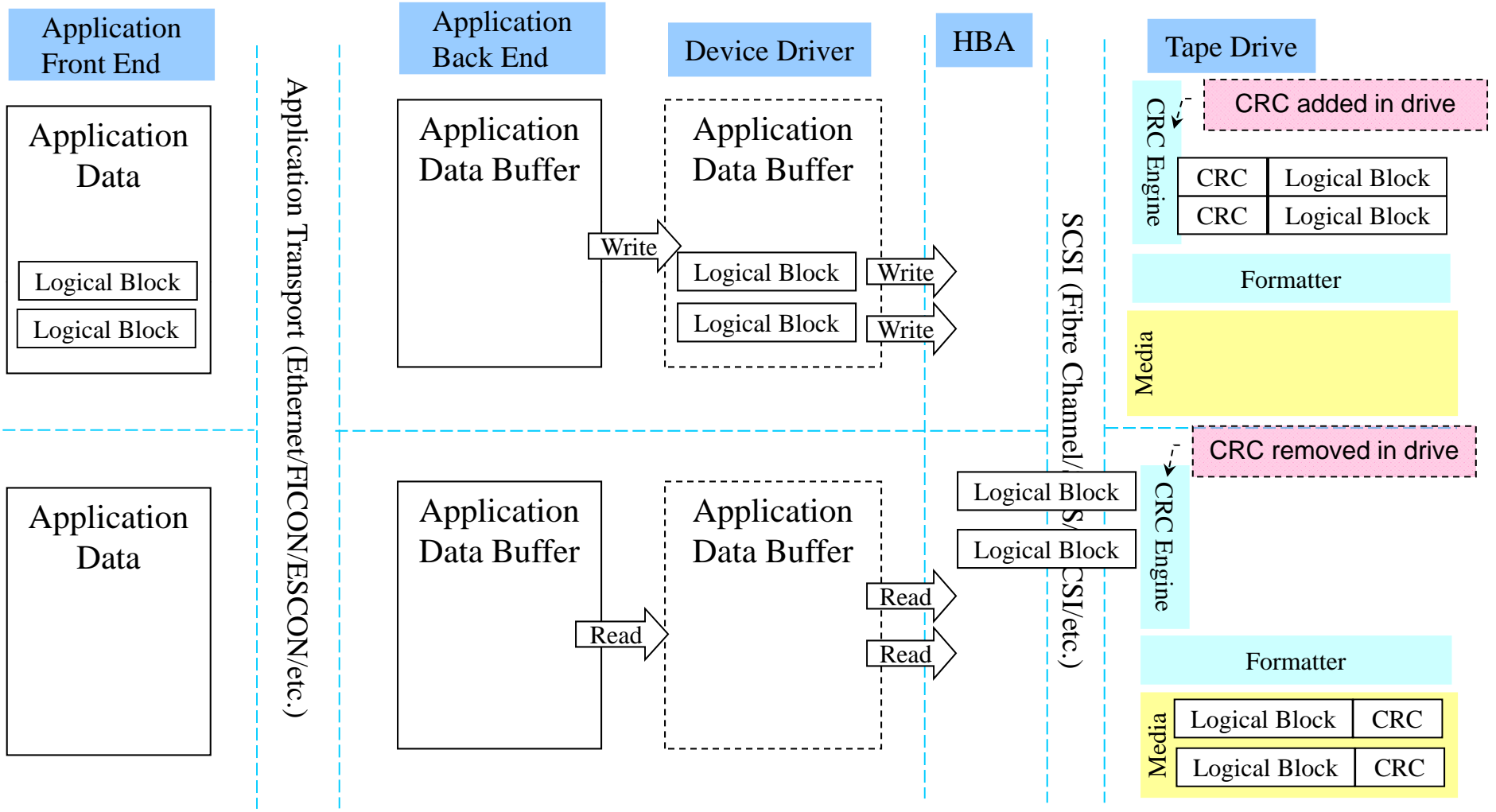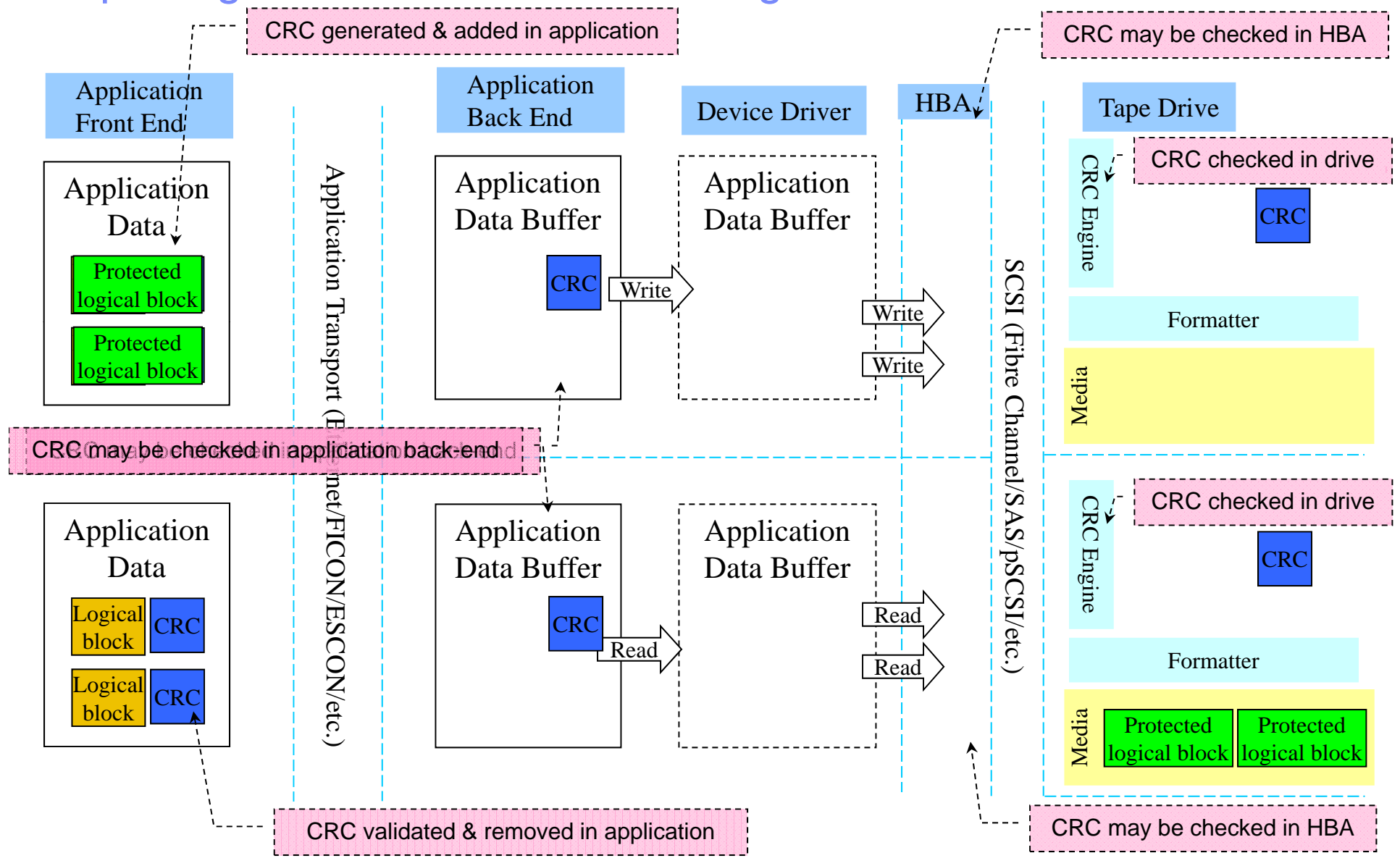
Tape Logical Block Protection

- Added to standards (SSC-4) in January 2010
- Write path is independent from Read path
  - Can read w/o CRC and can write with CRC
  - Can write w/o CRC and can read with CRC
  - Can write w/o CRC and can read w/o CRC
  - Can write with CRC and can read with CRC
- CRC is generated/checked at each end
  - Tape drive
  - Application
- CRC may be checked at any point along the path
  - HBA
  - Any system/software that is in the middle

Tape Logical Block Protection (cont)

- **On WRITE** (example in top half of following animated slide)
  - CRC is appended to each logical block at the source
  - CRC is checked at any point desired in the transfer
    - If corruption occurs, the exact location of problem is known
  - The logical block with CRC is validated before being committed to media
    - Data is known on to be on tape in uncorrupted form prior to releasing the source data
  - CRC is stored with each logical block
- **On READ** (example in bottom half of following animated slide)
  - logical block with the CRC is read and validated
  - CRC transferred with each logical block
  - CRC is check at any point desired in the transfer
  - The CRC is validated and stripped at the destination

Tape Logical Block Protection using SSC-4 method

This is an animated slide

CRC generated & added in application

CRC may be checked in HBA

Application Front End

Application Back End

Device Driver

HBA

Tape Drive

CRC checked in drive

CRC

Application Data

Protected logical block

Protected logical block

Application Transport (Ethernet/FICON/ESCON/etc.)

Application Data Buffer

CRC | Write →

Application Data Buffer

Write →

Write →

CRC Engine

Formatter

Media

SCSI (Fibre Channel/SAS/pSCSI/etc.)

CRC may be checked in application back-end

Application Data

Logical block | CRC

Logical block | CRC

Application Data Buffer

CRC | Read →

Read →

Application Data Buffer

Read →

Read →

CRC checked in drive

CRC

CRC Engine

Formatter

Media

Protected logical block | Protected logical block

CRC validated & removed in application

CRC may be checked in HBA

Logical Block Protection – VERIFY features

- Uses the VERIFY command defined in SSC-4
- Adds new options to:
  - Check that protection information (i.e., CRC) is the same as currently configured
    - Used in conjunction with other new options
  - Check that protection information (i.e., CRC) validates on each logical block from current position for n number of files (i.e., FMKS)
    - No blocks are transferred over the SCSI interface
    - Happens at native data rate
  - Check that protection information (i.e., CRC) validates on each logical block from current position to EOD
    - No blocks are transferred over the SCSI interface
    - Happens at native data rate

Logical Block Protection – VERIFY to EOD example