Data Integrity Proposal

Ver. 03/07/03

Agilent

Intel

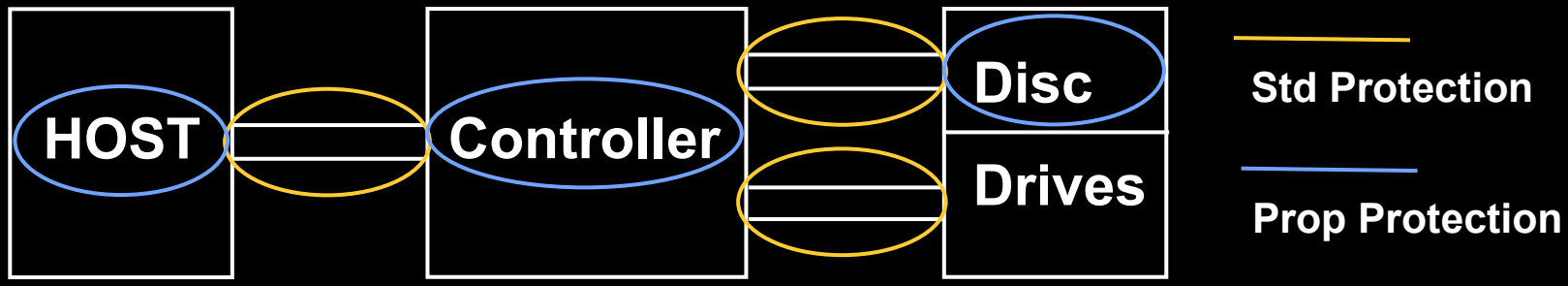
LSI Logic

Data Integrity – Today's Problem

Data Integrity checking has been implemented in some current Storage Systems.

- Implementations are not consistent or standardized
- Non-standard application-specific data sometimes allowed
- Limited, proprietary checking or verification is done in the Disc Drive

Current Industry Practice - 1



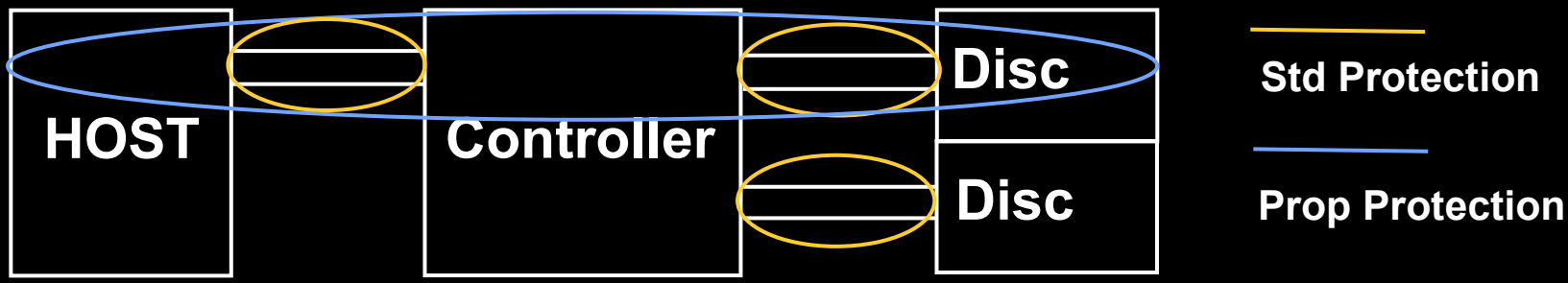
Host – Controller – Storage Model

- Standardized protection defined for Interfaces
- Each component has proprietary protection schemes

System philosophy is “check and regenerate” protection for each region.

Disadvantage: Opportunities for undetected corruption can occur during check and regenerate processes.

Current Industry Practice - 2



Host – Controller – Storage Model

Host can add proprietary protection bytes (end-to-end protection) to each block written to disc and recheck on read.

Disadvantage: Intermediate devices cannot check, just pass through. If error is seen, recovery is difficult or impossible. Also difficult to determine source of error. Timeframe may be long between error occurrence and discovery.

Solution: End-to-End Data Protection from Host to Drive

Implement a Standard Approach for End-to-End Data Protection

Support Data Protection Checks in Intermediate Controllers and Drives

Allow Application-Specific Data or Functions

Terminology

- Data Integrity Field (DIF) – Combination of Tag Data and Guard Fields
- Incrementing Tag Data – Used to validate that data is sent in correct order, with no duplicates, and that all data is transferred. The initial value of the Tag is specified in the CDB. Use of the Incrementing Tag is specified in CDB and may be turned ON or OFF from command to command.
- Fixed Tag Data – Fixed value is specified in CDB (e.g. Constant could be a logical unit number in a RAID system).
- Guard Field – Method of verifying (by calculating and comparing data checking algorithm) that correct data is transferred from interface to disk media, or from memory (could cross page boundaries) to the interface.

Data Integrity - Approach

- Generic Host-to-Drive Data Format
  - Standard block of data, length defined as Logical Block Size (LBS)
  - Application-Specific Data, where field length is included in LBS
  - 8-Byte Data Integrity Field (in addition to LBS)

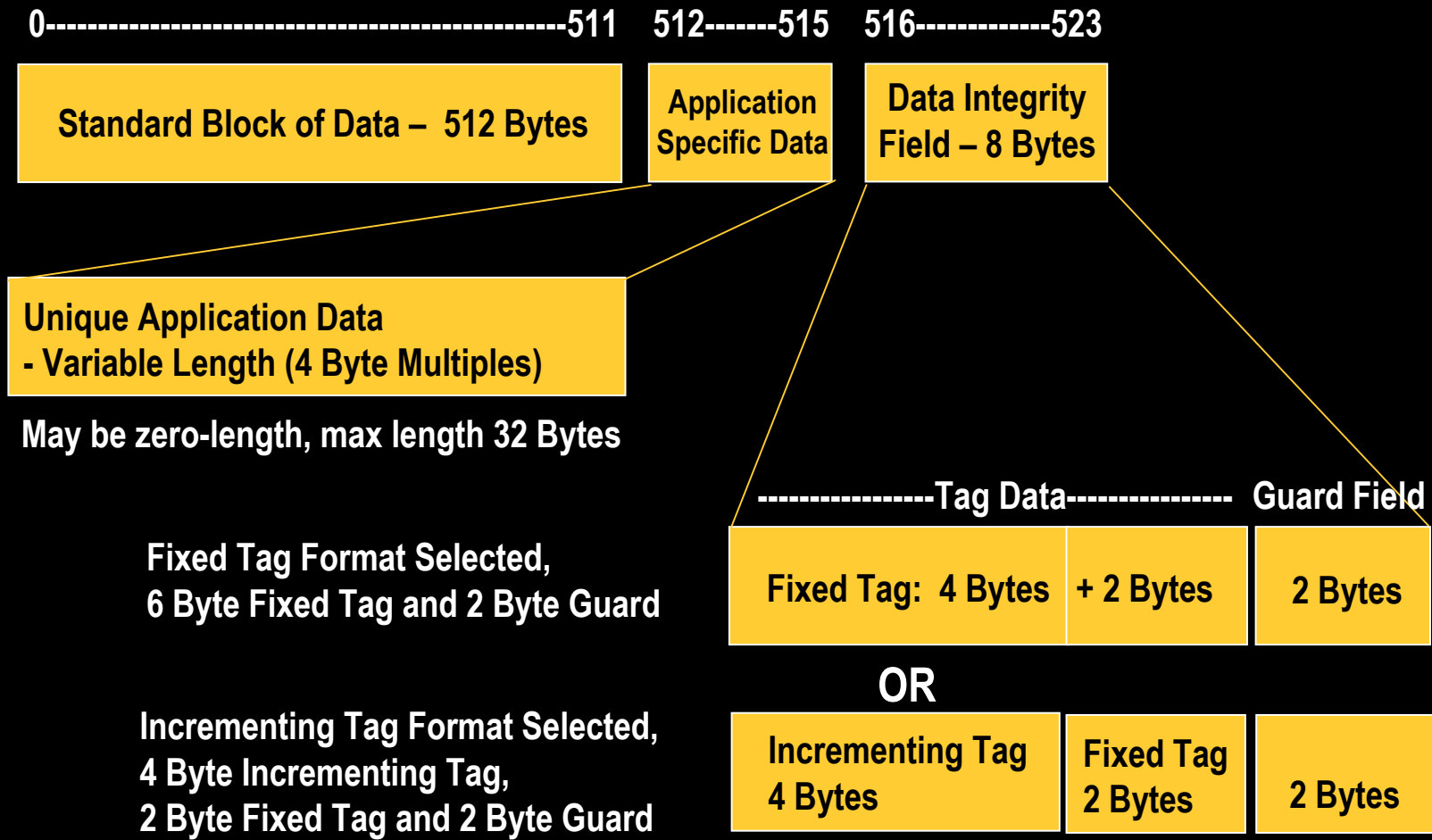
- Application-Specific Data
  - e.g. Software Stamp to indicate creator, data type, creation and/or last modification date, data path, or other identification information.

- Data Integrity Field (DIF)
  - Data Integrity Field includes Tag Data and Guard field.

- New CDBs for this new Data type
  - Read / Write / Verify / Write & Verify / Write Same
  - New Op Codes (16-Byte structure)

Generic Data Format – Host to HDD

Total allowable length - up to 4096 Bytes, including ASD and DIF



Data Integrity Configuration Settings

The Data Integrity Mode Page is used to specify configuration settings and data that will not change from command to command.

The Command Descriptor Block (CDB) is used to specify configuration settings and data that may change from command to command.

Data Integrity Mode Page

Store Data Integrity Field (STOR_DIF) – affects sector format

- Total length of Data Stream (LBS + DIF) must be written to (or read from) media

Specify Type of Guard Field to be Generated or Verified

- Guard = None
- Guard = simple, fast computation (in HW or FW)
- Guard = able to detect data displacement errors

Specify Data Range for Calculation of Guard

- LBS, including Application Specific Data (no exclusion)
- LBS, with all, or a portion, of ASD field excluded

Specify Defaults for Tag Data Fields

- Used to fill in Tag Data and Guard fields with Legacy CDBs

(DIF Field is not transferred across Interface with Legacy CDBs)

16 Byte CDB w Tag Data

	Bit							
Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (TBD)							
1		RESERVED		DPO	FUA	CHK_OPTN		INCR/FIX
2								
3								
4								
5								
6								
7								
8								
9								
10	(MSB)	FIXED TAG DATA						
11		(2 Bytes)						(LSB)
12	(MSB)	TRANSFER LENGTH						
13		(2 Bytes)						(LSB)
14	RESERVED							(LSB)
15	CONTROL							

LongLBA – Specifies 8 Byte LBA, where 4 Byte Tag serves as part of LBA.

CHK_OPTN – Allows disabling of Tag Data and Guard field verification.
(Mode Page specifies type of Guard).

INCR/FIX – Indicates type of Data contained in 4-Byte Incrementing/Fixed Tag Data field.

INCREMENTING TAG FIELD – Contains 4-Byte Incrementing or Fixed Tag Data value.

FIXED TAG FIELD – Contains 2-Byte Fixed Tag Data value.

DIF Write Operation Sequence

- Host generates Guard value at the Application, Driver, or HBA levels. Data Stream includes DIF Field for each Logical Block.
- Hosts communicates format (Fixed and/or Incr) and value of Tag Fields in the CDB.
- For each block, verification is done at Intermediate Controller and Target Device.
  - Guard value calculated and compared to Host value
  - Verify Tag Fields in CDB compare to Data Stream
  - Write operation halts when error is detected

DIF Read Operation Sequence

- For each block, verification will be done at Target, Intermediate Controller and Host Devices.
  - Guard value calculated and compared to value in Data Stream
  - Tag Fields in CDB are compared to Data Stream
  - Read operation halts when error is detected

Legacy Write Operation Sequence

- Host generates Data Stream at the Application level. Block of Data with no DIF Field for each Logical Block.
- When STOR_DIF flag set, DIF Field is inserted at Intermediate Controller or Target.
- For each Block of Data, DIF verification is done at points after DIF insertion point.
  - Guard value calculated and compared to Data Stream
  - Verify Tag Fields in CDB compare to Data Stream
  - Write operation halts when error is detected

Legacy Read Operation Sequence

- For each Block of Data, verification is done at Target and Intermediate Controller (prior to DIF removal point).
  - Guard value calculated and compared to value in Data Stream
  - Tag Fields in CDB are compared to Data Stream
  - Read operation halts when error is detected
- When STOR_DIF flag set, DIF Field is removed by Target or Intermediate Controller.

Error Handling

- Specific Error cases and Methods of Handling those cases will need to be defined prior to release of a standard.
- This feature creates a new type of error not previously considered in the T-10 standard. A new subclass of error code (e.g. 03/11/xx) is required to indicate a system error condition as opposed to a drive or interface error.

Benefits

Primary benefits of a cooperative scheme:

- Data Integrity information is written to the drive media to provide end to end assurance of data integrity.
- Detection of data failures at the drive level is enabled during write operations and read operations.
- Isolation / Correction of bad data occurs as early as possible, with minimum impact to system integrity and performance.
- Standard approach results in common methodology between vendors to ease management and maintenance for customers.
- Flexibility to allow Application-Specific Data, and options for Data Integrity checks, provide varied implementation possibilities for end-users.