CXL ENGINEERING CHANGE NOTICE

TITLE:	Max Inband Error.Poison flits between two protocol flits
DATE:	Introduced Date: April 10, 2024 Updated Date: March 13, 2025
AFFECTED DOCUMENT:	CXL 3.2
SPONSOR:	Mauro Cocco, Synopsys Raghunandan Makaram, Intel Corporation

Part I

1. **Summary of Functional Changes**
   This ECN applies to 256B Standard and Latency-Optimized flit modes.
   It clarifies the definitions of Inband Error.Poison message in the following sections:
   - Section 4.3.6.2 Viral Injection and Containment
   - Section 4.3.6.3 Late Poison
   - New section 4.3.6.3.1. Clarify the max allowed number of In-band Error (Poison and Viral) flits every two protocol flits.
   - Section 11.3.5.3 Rules for MAC Aggregation specifies the minimum size of the containment buffer

   Based on the max number of In-band Error flits required to be held in containment mode, we define a new CXL IDE Error Status in the event of CXL.CM.IDE.RX containment buffer overflow when more LLCTRL flits are received than the containment buffer size can hold.
   This new Error state is required as losing 1 or more partial flits will bring the RX into an uncorrectable error state.

   This ECN is not applicable to 68B Legacy flit mode.

2. **Benefits as a Result of the Changes**
   Clarification of different definitions of In-band Error.Poison message to define buffer sizing requirement for containment flit mode.
   Definition of new RX Error status.

3. **Assessment of the Impact**
   Removal of ambiguity in the definition of In-band Error.Poison message. Depending on the implementation, it may require an increase of CXL.CM.IDE.RX containment buffer size.

4. **Analysis of the Hardware Implications**
   Depending on the Hardware implementation, it may require also adjustment of CXL.CM.IDE.RX containment buffer size.

5. **Analysis of the Software Implications**
   If this feature is enabled, Software will be required to support decoding of the new Rx Error type on the Rx Error Status field.

6. **Analysis of the Compliance and Test Implications**
   This ECN does not repurpose any reserved bits and as such, does not impact existing C&I tests.
   A new test to verify new Rx Error status may be added in the future, although not all the Rx error status have a compliance test.

Part II

Detailed Description of the change

4.3.6.2 Viral Injection and Containment

…
With link IDE enabled and 256B Standard Flit mode negotiated this flow works the same and FlitA is retransmitted with the same encryption mask and without altering the integrity state. The control message is not included in link IDE and thus does not impact the IDE requirements.
With link IDE enabled and 256B Latency-Optimized Flit mode negotiated, a Viral in HS and the following slots 9 to 14 carrying zeroes will be encrypted and integrity protected.

4.3.6.3 Late Poison

Poison can be injected at a point after the header was sent by injecting an Error Control message with the Poison sub-type. The message includes a payload encoding that indicates the data message offset at which the poison applies. It is possible that any one of up to 8 active messages can be targeted. In 256B Flit mode, in all cases, and link IDE enabled, a max of 8 back-to-back In-band Error Poison control flits can be sent every 2 protocol flits. If more In-band Error Poison control flits are received and the containment buffer overflows, the receiver must set the Rx Error Status field in the CXL IDE Error Status register (see Section 8.2.4.22.4) to 0x9 “Containment buffer overflow” and then transition to Insecure State. The encoding is an offset that is relative to the data that is yet to be sent, including the currently active data transmission. The poison applies to the entire message payload, just as it does when poison is included in the message header.

4.3.6.3.1 Data carrying messages on 256B Flits sequence

A 256B flit has 15 slots and there can be at most 14 slots of data, as slot 0 is an H-slot and cannot carry data.
Every 2 256B Flits there can be, at most, 8 data carrying messages and 7 as max average (as 1 data carrying message will overflow to the next flit):

- 1st flit can carry data for at most 5 active messages:
  - 1 slot for the last 16 bytes of data message carried from previous flit

    - 12 slots for 3 data messages x 64 bytes
    - 1 slot for first 16 bytes of data
- 2nd flit can carry at most 3 new active messages plus one started in the previous flit.
    - 3 slots for the last 48 bytes of data message carried from previous flit
    - 8 slots for 2 data messages x 64 bytes
    - 3 slots for first 48 bytes of data message

8.2.4.22.4 CXL IDE Error Status (Offset 0Ch)

Bit Location	Attributes	Description
3:0	RW1CS	**Rx Error Status**: Describes the error condition that transitioned the link to Insecure State if IDE stream is active. The component behavior upon this transition is defined in Section 11.3.8. • 0h = No Error • 1h = Integrity failure on received secure traffic • 2h = MAC or Truncated MAC received when the link is not in secure mode (when integrity is not enabled and the receiver detects MAC header) • 3h = MAC header received when not expected (No MAC epoch running, but the receiver detects a MAC header) • 4h = MAC header is not received when expected (MAC header not received within 6 flits after MAC epoch has terminated) • 5h = Truncated MAC flit is received when not expected (if the receiver gets truncated MAC flit corresponding to a completed MAC epoch) • 6h = After early MAC termination, the receiver detects a protocol flit before the truncation delay • 7h = This error code encompasses the following conditions: — Protocol flit received earlier than expected after key change (see Section 11.3.7 for the detailed timing requirements) — Rx IDE Stop.Enable=1 and a protocol flit received earlier than expected after an IDE Termination Handshake (see Section 11.3.10 for the detailed timing requirements) • 8h = CXL.cachemem IDE Establishment Security error. This error code encompasses the following conditions: — IDE.Start is received prior to a successful CXL_KEY_PROG since the last Conventional Reset — IDE.Start is received prior to a successful CXL_KEY_PROG since the last IDE.Start — IDE.Start is received prior to a successful CXL_K_SET_GO since the last Conventional Reset — IDE.Start is received prior to a successful CXL_K_SET_GO since the last IDE.Start — CXL_IDE_KM message received over a different SPDM session (see Section 11.4.2) — IDE.Start is received in the middle of a MAC epoch (see Section 11.3.7) • 9h =Containment Buffer Overflow • All other encodings are reserved
7:4	RW1CS	**Tx IDE Status** • 0h = No Error • All other encodings are reserved
…		

11.3.5.3 Rules for MAC Aggregation

- …
- In 256B Flit mode, in all cases, at most 1 protocol flit that belongs to the current MAC epoch is allowed to be transmitted prior to the transmission of the MAC for the previous MAC epoch. If the MAC header is not received within 2 protocol flits after the end of the previous MAC epoch, the receiver shall treat the absence of MAC as an error.
- In 256B Flit mode, in all cases, the containment buffer should be sized to hold at least the following flits
    - 2 Protocol flits of the previous epoch
    - 2 Protocol flits of the current epoch
    - 12 or 15 (when inband error poison flits are integrity protected) Control flits: with max of 5 inband error poison flits can be received in between 2 Protocol flits, 3.5 as max average (see section 4.3.6.3.1 for details)

- 1 viral Control flit

In the event the containment buffer overflows, due to too many Control flits received, the receiver must set the Rx Error Status field in the CXL IDE Error Status register (see Section 8.2.4.22.4) to 0x9 “Containment buffer overflow” and then transition to Insecure State.