CXL ENGINEERING CHANGE NOTICE

TITLE:	ECN to add late poison message protection with IDE and new device capabilities for handling late poison
DATE:	Introduced date (03/28/2024) Updated date (05/22/2024)
AFFECTED DOCUMENT:	CXL 3.1
SPONSOR:	Chet Douglas, Intel Corporation Makaram Raghunandan, Intel Corporation

Part I

- **Summary of Functional Changes**
  Add IDE protection for late poison messages and new capabilities and control bits for handling late poison target behavior

- **Benefits as a Result of the Changes**
  Authenticate late poison messages using IDE

- **Analysis of the Hardware Implications**
  There may be hardware implications for this ECN

- **Analysis of the Software Implications**
  There may be software implications for this ECN

- **Analysis of the Compliance and Test Implications**
- Unaffected

Part II
Detailed Description of the change

Add the following new section 11.3.11 Poison Handling

11.3.11 Poison handling

The CXL.cachemem protocol has two mechanisms for conveying poison:

- Use the poison bit in the headers that have poisoned data associated with them (see the poison bit in the CXL.cache D2H Data Header, H2D Request and the CXL.mem flit definitions).
- Utilize 256 byte flits with the LLCTRL message with Subtype Poison. This message can be carried in an H slot for standard flits and in an H or HS slot for LOpt flits (see the link layer Late Poison description in section 4.3.6.3). The LLCTRL message includes a payload encoding that indicates the data message offset where the poison applies. Since multiple data messages can be outstanding at the same time, there can be multiple in-band LLCTRL Poison messages outstanding at the same time.

In general, IDE does not apply to LLCTRL messages. However, the Poison message needs to have integrity protection by CXL.cachemem IDE. Otherwise, an adversary can inject/delete an in-band LLCTRL Poison message without detection by IDE. Injection of a LLCTRL Poison message is not a concern as it only impacts the availability of the TCB (which an adversary has many other simpler ways to achieve). However, deleting or modifying an in-band LLCTRL Poison message is problematic as it can lead to silent consumption of data that should have been poisoned.

When LLCTRL Poison is present in the H slot of a flit, the payload information of the message shall be treated as additional bits of AAD. There are 4 bits of payload defined in the specification. Each LLCTRL Poison message shall result in 32 bits of AAD (4 bits of payload along with 28 bits of padding). The remaining slots of the flit carrying the poison indication shall be considered reserved and those slots shall not be encrypted, or integrity protected. This AAD value shall be treated as additional AAD for the next protocol flit. Thus, the flit carrying LLCTRL Poison in the H slot does not count towards MAC Epoch (see Figures x1 & x2 below). The MAC Epoch is still defined based on the protocol flits. Since the poison payload is incorporated into the integrity calculations as AAD, it can be authenticated without impacting IDE encryption.

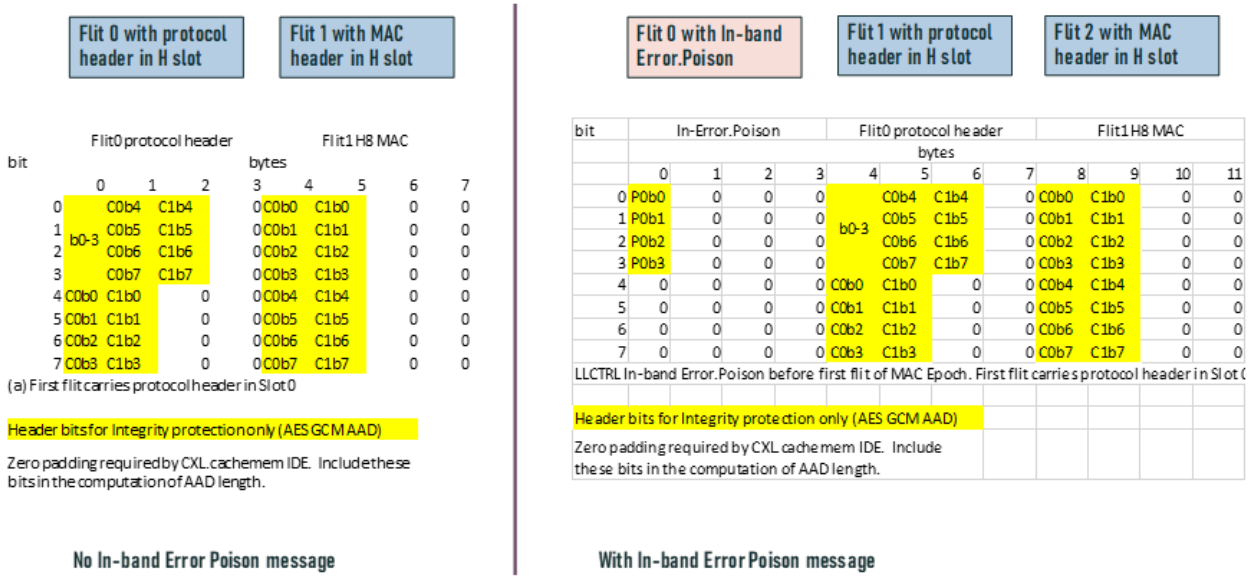

Figure X1 Containment Mode example illustrating the AAD construction for the case of two protocol flits that are part of the current MAC Epoch with an in-band LLCTRL Poison sent prior to first flit of the MAC Epoch.

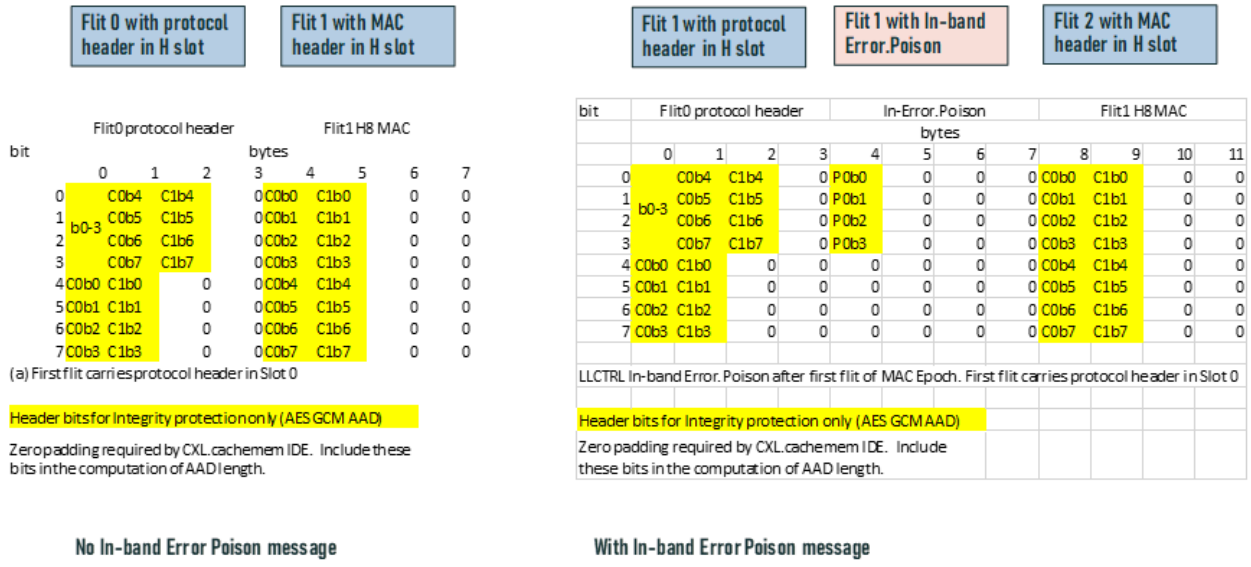

Figure X2 Containment Mode example illustrating the AAD construction for the case of two protocol flits that are part of the current MAC Epoch with an in-band LLCTRL Poison message sent after first flit of the MAC Epoch.

When a LLCTRL Poison message is present in an HS slot of a flit, and the rest of the flit already contains valid protocol information, then there is no change required to the current IDE definition as the HS slot is already authenticated.

11.3.11.1 Late poison with CRC corruption flow

There is a variant of late poison in the case where all of the data that needs to be poisoned is packed into the current flit (see the link layer Late Poison description in section 4.3.6.3). In this case, the CRC of the flit is corrupted before transmission. This ensures a retry condition will be triggered. When the retry request is received, the LLCTRL Poison message is sent first, followed by the original flit, without CRC corruption. The approach described previously will work with the late poison flow for standard flits and LOpt flits where the CRC of the first half of the flit is corrupted and the LLCTRL Poison message is carried in the H slot of the flit. The transmitter shall ensure that the original flit with the corrupted CRC, the LLCTRL Poison flit, and the original flit with good CRC are sent sequentially, with no intervening protocol flits. The transmitter shall also ensure that the MAC for the current MAC Epoch that includes the CRC corrupted flit is not transmitted ahead of the CRC corruption flow, as the MAC will need to be recomputed to include the AAD values from the LLCRTL Poison payload.

As noted in Viral Injection and Containment *(add reference to section 4.3.6.2)*, IDE cannot be supported with the LOpt flit with CRC corruption of the second half of the flit. When IDE is enabled, any error containment shall be either detected sufficiently early enough to corrupt the CRC of the first half of flit or must be injected as an HS slot LLCTRL Poison message without needing to corrupt the CRC of the second half of the flit.

11.3.11.2 Support of authenticated LLCTRL Poison messages

Devices supporting the inclusion of the LLCTRL Poison message in the AAD shall declare support by setting the IDE Protect LLCTRL Poison Message Capable bit in the CXL IDE Capability register. Hosts wishing to enable this feature on the device shall set the IDE Protect LLCTRL Poison Message Enable bit in the CXL IDE Control register.

Add the following changes to section 8.2.4.22.1 CXL IDE Capability

Bit Location	Attributes	Description
23	HwInit/RsvdP	**LOpt IDE Capable**: If set, this component supports IDE when the link is operating in Latency-Optimized 256B Flit mode (see Figure 11-13 and Figure 11-14).2If 0, this component does not support IDE when the link is operating in Latency-Optimized 256B Flit mode. If the link is operating in Latency-Optimized 256B Flit mode, the System Firmware or System Software must clear the CXL_Latency_Optimized_256B_Flit_Enable bit the DVSEC Flex Bus Port Control register (see Section 8.2.1.3.2) in the Downstream Port and then retrain the link prior to enabling IDE. After IDE is terminated, the System Firmware or System Software may set the CXL_Latency_Optimized_256B_Flit_Enable bit in the Downstream Port and then retrain the link so that the link can transition to Latency-Optimized 256B Flit mode.
24	HwInit/RsvdP	**IDE Protect LLCTRL Poison Message Capable**: If set, this component supports IDE protection of LLCTRL In-band Error poison information.
31:~~24~~25	RsvdP	**Reserved**

Add the following changes to section 8.2.4.22.2 CXL IDE Control

Bit Location	Attributes	Description
0	RW	**PCRC Disable**: When set, PCRC generation is disabled and MAC calculation does not include PCRC. Software must ensure that this bit is programmed consistently on both ends of the CXL link. Changes to this bit when CXL.cachemem IDE is active results in undefined behavior. The default value of this bit is 0.
1	RW/RsvdP	**IDE.Stop Enable**: Enables generation of IDE.Stop control flit by the port Tx and processing of IDE.Stop control flit by port Rx when operating in 256B Flit mode.1This bit must be RW if the IDE Stop Capable bit is set; otherwise, it is permitted to be hardwired to 0. Software must not set this bit unless the IDE.Stop Capable bit is set to 1. The default value of this bit is 0
2	RW/RsvdP	**IDE Protect LLCTRL Poison Message Enable**: Enables IDE protection of LLCTRL In-band Error poison. The bit must be RW if IDE Protect LLCTRL Poison Message Capable bit is set. Software must not set this bit unless both ends of the link have the IDE Protect LLCTRL Poison Message Capable bit set. Default value of this bit is 0.
31:~~2~~3	RsvdP	Reserved