What is the difference between the Emergency Operation Time Interval (EOTI) and the Emergency Operation Tolerance Time Interval (EOTTI), and how do these support the transition to a safe state?

The Emergency Operation Time Interval (EOTI) and the Emergency Operation Tolerance Time Interval (EOTTI) are distinct time-spans defined in ISO 26262 that are crucial for managing risks and achieving a safe state after a fault occurs in an item.

**Emergency Operation Time Interval (EOTI)**
The Emergency Operation Time Interval (EOTI) is defined as the time-span during which emergency operation is maintained (ISO 26262-1:2018 Clause 3.44). Emergency operation is a temporary state where safety is maintained until the transition to a safe state is achieved (ISO 26262-1:2018 Clause 3.44 Note 3). This interval represents the actual duration for which the system operates in a degraded or alternative mode following a fault, before reaching its final safe state.

**Emergency Operation Tolerance Time Interval (EOTTI)**
The Emergency Operation Tolerance Time Interval (EOTTI) is the specified time-span during which emergency operation can be maintained without an unreasonable level of risk (ISO 26262-1:2018 Clause 3.45). It is the maximum allowable value for the emergency operation time interval (ISO 26262-1:2018 Clause 3.45 Note 2). Emergency operation is considered safe within this interval due to its limited duration (ISO 26262-1:2018 Clause 3.45 Note 3). To minimize risk, the emergency operation time interval is limited by the EOTTI, which is defined as part of the safety concept (ISO 26262-10:2018 Clause 12.2.4.3).

**How they support the transition to a safe state**
These time intervals are integral to the warning and degradation strategy of an item and support the transition to a safe state in the following ways:

1. **Response to Faults when Safe State is not immediate:** An emergency operation is specified when a safe state cannot be reached within the Fault Tolerant Time Interval (FTTI) (ISO 26262-10:2018 Clause 4.4.1). The FTTI is the minimum time from fault occurrence to a possible hazardous event if safety mechanisms are not activated (ISO 26262-1:2018 Clause 3.61). Emergency operation is initiated before the FTTI expires and is maintained until the safe state is reached, which must occur before the end of the EOTTI (ISO 26262-10:2018 Clause 4.4.1).
2. **Risk Mitigation during Degraded Operation:** During emergency operation, the item is still free from unreasonable risk (ISO 26262-10:2018 Clause 12.2.4.1). Even if the ASIL capability of the item in this state is lower than the ASIL rating of the potential hazard, the operating time in this state is limited by the EOTTI. This limitation ensures it is unlikely that an additional fault occurs which could lead to a violation of the safety goal (ISO 26262-10:2018 Clause 12.2.4.1). The emergency operation time interval itself can be considered free from unreasonable risk not due to achieved risk reduction, but because the item spends a limited time in this operating state (ISO 26262-10:2018 Clause 12.2.5.5).
3. **Ensuring Safety Goal Fulfillment:** To meet the safety goal, a safe state must be reached before the end of the emergency operation tolerance time interval (ISO 26262-10:2018 Clause 4.4.1). The EOTTI represents the maximum allowable time to reach this safe state (ISO 26262-10:2018 Clause 12.2.5.5).
4. **Quantitative Analysis and Design Consideration:** The EOTTI is defined and verified based on the probability of a subsequent fault (ISO 26262-10:2018 Clause 12.2.4.1 Note 1). For systems using redundancy to achieve fault tolerance, if the ASIL capability of the system in an operating mode without redundancy does not meet the required ASIL, the EOTTI limits the allowable time in this state to reduce the risk of a second fault (ISO 26262-10:2018 Clause 12.3.1.1). Quantitative analysis, such as PMHF (Probabilistic Metric

for Random Hardware Failures) estimation, can be used to calculate a limit for the EOTTI to prevent safety goal violation from a subsequent random hardware fault (ISO 26262-10:2018 Clause 12.3.1.1, ISO 26262-10:2018 Clause 12.3.1.1). When determining the EOTTI, considerations include physical system limitations, additional safety requirements for hardware and software elements used during emergency operation, and the possibility of common cause failures in the remaining system (ISO 26262-10:2018 Clause 12.2.4.3 Note 1).

In essence, EOTI is the actual time spent in emergency operation, while EOTTI is the maximum permissible time to ensure that safety goals are met and unreasonable risk is avoided until a stable safe state is achieved.

**Additional list of Clauses:**

- ISO 26262-1:2018 Clause 3.44 emergency operation time interval
- ISO 26262-1:2018 Clause 3.44 Note 3 to entry
- ISO 26262-1:2018 Clause 3.45 emergency operation tolerance time interval
- ISO 26262-1:2018 Clause 3.45 Note 2 to entry
- ISO 26262-1:2018 Clause 3.45 Note 3 to entry
- ISO 26262-1:2018 Clause 3.61 fault tolerant time interval
- ISO 26262-10:2018 Clause 4.4.1
- ISO 26262-10:2018 Clause 12.2.4.1 Emergency operation
- ISO 26262-10:2018 Clause 12.2.4.1 Note 1
- ISO 26262-10:2018 Clause 12.2.4.3 Emergency operation time interval
- ISO 26262-10:2018 Clause 12.2.4.3 Note 1
- ISO 26262-10:2018 Clause 12.2.5.5 Flow of events for this example
- ISO 26262-10:2018 Clause 12.3.1.1 Emergency Operation Tolerance Time Interval calculation method

Correctness 4P, -1P ambigouse wording of emergency operation time interval regarding  free from unreasonable risk not
Completness 5P