An engineer is working on a component originally allocated an ASIL C safety requirement. To reduce development complexity, he decides to implement the functionality using two redundant elements developed to ASIL B(C). Is this decomposition strategy compliant with ISO 26262, and what might be their reasoning behind this choice?

Yes, this decomposition strategy is generally compliant with ISO 26262, provided certain conditions are met, and there are clear reasons why an engineer might choose this.

Compliance with ISO 26262:

According to ISO 26262-9:2018, Clause 5.4.9 b), for an ASIL C requirement, the permitted decomposition schemas are:

1. one ASIL B(C) requirement and one ASIL A(C) requirement; or
2. one ASIL C(C) requirement and one QM(C) requirement.

While "ASIL B(C) and ASIL B(C)" is not explicitly listed as one of the options for ASIL C in Clause 5.4.9 b), the standard also states that "A decomposition schema resulting in higher ASILs may also be used" (ISO 26262-9:2018, Clause 5.4.9). In this case, comparing "ASIL B(C) and ASIL B(C)" to the allowed "ASIL B(C) and ASIL A(C)", one of the resulting ASILs (ASIL B(C)) is indeed higher than ASIL A(C). Therefore, the chosen decomposition is more stringent or equally stringent for individual elements than one of the explicitly allowed options and is permissible under this rule.

Key Requirements for any ASIL Decomposition:

For this decomposition to be valid, several critical requirements from ISO 26262-9 must be met:

- **Sufficient Independence:** The two redundant elements, developed to ASIL B(C), must be sufficiently independent. This means that an analysis of dependent failures (see ISO 26262-9:2018, Clause 7) should not find a plausible cause of dependent failures that could lead to the violation of the initial ASIL C safety requirement, or any identified cause must be controlled by an adequate safety measure (ISO 26262-9:2018, Clause 5.4.3, Clause 5.4.10).
- **Individual Compliance:** Each decomposed safety requirement (i.e., each ASIL B(C) requirement) shall be capable of complying with the initial ASIL C safety requirement by itself, providing redundancy by definition (ISO 26262-9:2018, Clause 5.4.4).
- **Systematic Faults:** ASIL decomposition is applied specifically in the context of systematic failures, aiming to reduce the likelihood of such failures (ISO 26262-10:2018, Clause 11.2).
- **Random Hardware Failures:** It is crucial to note that ASIL decomposition does not apply to requirements specific to random hardware failures, including the evaluation of hardware architectural metrics and safety goal violations due to random hardware failures. These requirements remain unchanged by ASIL decomposition (ISO 26262-1:2018, Clause 3.3 Note 2; ISO 26262-9:2018, Clause 5.2; ISO 26262-9:2018, Clause 5.4.5; ISO 26262-10:2018, Clause 11.2).

Reasoning Behind the Choice (ASIL B(C) and ASIL B(C)):

The engineer's reasoning behind this choice is aligned with the general objectives and benefits of ASIL decomposition:

- **Reduced Development Complexity/Rigour:** The primary objective of ASIL decomposition is "to assign a potentially lower ASIL to (some of) these decomposed safety requirements" (ISO 26262-9:2018, Clause 5.2). By decomposing an ASIL C requirement into two ASIL B requirements, the development rigor and the necessary ISO 26262 requirements and safety measures for each individual element are reduced from ASIL C to ASIL B (ISO 26262-1:2018, Clause 3.6). This can simplify the design, implementation, and verification activities for each element (ISO 26262-9:2018, Clause 5.4.11).

- **Achieving Safety Goal with Redundancy:** The objective of ASIL decomposition is "to comply with the safety goal by using multiple sufficiently independent elements with respect to systematic faults" (ISO 26262-10:2018, Clause 11.1). By implementing the functionality with two redundant, independent elements, the overall safety goal can still be achieved even if one element fails. The strategy ensures that "the initial safety requirement shall be decomposed to redundant safety requirements, that shall be implemented by sufficiently independent elements" (ISO 26262-9:2018, Clause 5.4.3).
- **Systematic Fault Mitigation:** ASIL decomposition is a method to manage systematic failures. By distributing the safety requirements across two independent ASIL B elements, the likelihood of a common systematic fault affecting both elements, leading to a safety goal violation, is intended to be reduced (ISO 26262-10:2018, Clause 11.2).
- **Design Flexibility:** ASIL decomposition offers flexibility in architectural design, allowing for the partitioning of ASIL requirements across elements (ISO 26262-9:2018, Clause 5.2).

In summary, the engineer's choice to decompose an ASIL C requirement into two ASIL B(C) requirements is generally compliant with ISO 26262, as it represents a more stringent approach than the minimum allowed (B(C) + A(C)) for one of the elements, and it aligns with the goal of reducing the development rigor for individual elements while maintaining overall safety through redundancy and independence.

Additional List of Clauses:

- ISO 26262-1:2018, Clause 3.3 ASIL decomposition
- ISO 26262-1:2018, Clause 3.6 automotive safety integrity level (ASIL)
- ISO 26262-9:2018, Clause 5.1 Objectives
- ISO 26262-9:2018, Clause 5.2 General
- ISO 26262-9:2018, Clause 5.4.3
- ISO 26262-9:2018, Clause 5.4.4
- ISO 26262-9:2018, Clause 5.4.5
- ISO 26262-9:2018, Clause 5.4.9
- ISO 26262-9:2018, Clause 5.4.9 b)
- ISO 26262-9:2018, Clause 5.4.10
- ISO 26262-9:2018, Clause 5.4.11
- ISO 26262-10:2018, Clause 11.1 Objective of ASIL decomposition
- ISO 26262-10:2018, Clause 11.2 Description of ASIL decomposition

Correctness = 4P, -1P unfurtunate choice of wording which leads to missunderstanding of dividing the safety requirements. Clarification would be using sigular so it is better understood.
Completness = 5P (It correctly saw that B +B equals higher)