Based on the given pattern, we will create a security case for an Instant Messaging (IM) software, defining specific terms and instantiating placeholders. Here's the assurance case and its hierarchical tree representation:

\*\*Security Assurance Case for Instant Messaging (IM) Software\*\*:

- Goal (G1, "IM software is acceptably secure in operational system")

- Context (C1, "Definition and description of IM software")

- Context (C2, "Definition and description of operational system")

- Context (C3, "Acceptably secure means the software can defend against known common vulnerabilities and ensures data privacy")

- Strategy (S1, "Argument that IM software assets are under protection")

- Justification (J1, "Protection of IM software assets supports that software is acceptably secure")

- Supported By

- Goal (G2, "All identified IM software critical assets are protected")

- Context (C4, "List of IM software critical assets: user data, authentication mechanisms, message store, transmission protocols")

- Strategy (S2, "Respective arguments of IM software critical assets")

- Justification (J2, "Relationship between assets is clear and can be argued separately")

- Supported By

- Goal (G3, "IM software critical asset is protected")

- Strategy (S3, "Argument of the type which the IM software critical asset belongs to: such as data at rest, data in transit")

- Context (C5, "List of IM software critical asset types in PEDD: User Data, Authentication Data, Configuration Data, Cached Data")

- Justification (J3, "Types of IM software assets are consistent with PEDD classification")

- Supported By

- Goal (G4, "IM software critical asset, User Data, which belongs to data at rest type is protected")

- Goal (G4, "IM software critical asset, Authentication Data, which belongs to data in transit type is protected")

- Goal (G4, "IM software critical asset, Configuration Data, which belongs to data at rest type is protected")

- Goal (G4, "IM software critical asset, Cached Data, which belongs to data in transit type is protected")

This hierarchy clearly outlines how the top-level security goal (G1) for the IM software being acceptably secure within the operational system is supported by multiple strategies and contexts, further broken down into sub-goals and respective strategies for each critical asset and type of asset. Each instance of G4 provides assurance for different types of critical assets being protected as per the defined contexts and justifications, which supports the overarching claim of security.