Based on the predicates and information provided for the Instant Messaging (IM) software domain, here is a hierarchical tree structure for the security case using Goal Structuring Notation (GSN):

```

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

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

Context (C2, "Definition and description of operational environment")

Context (C3, "Definition of acceptably secure")

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

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

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

Context (C4, "List of IM software critical assets: Registration info, Registration process, User account info, Authentication info, Login process, Chat logs")

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

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

Goal (G3, "Each software critical asset is protected")

Strategy (S3, "Argument of the type which the software critical asset belongs to")

Context (C5, "List of software critical asset types in PEDD: Process, Environment Entity, Data Exchange, Data Storage")

Justification (J3, "Types of software assets are according to PEDD")

Goal (G4, "Software critical asset which belongs to type is protected (Multiple Instances)").

```

Explanation:

- \*\*G1\*\* is the top-level goal stating the primary objective is to ensure the IM software is secure in a specific operational environment.

- \*\*C1, C2, C3\*\* provide necessary background and definitions relating to the software, the system it operates within, and what "acceptably secure" means in this context.

- \*\*S1\*\* strategizes that the argument for achieving G1 rests on showing all assets are protected.

- \*\*J1\*\* justifies that protecting the assets supports the primary claim that the software is secure.

- \*\*G2\*\* further narrows down the focus to ensuring all critical assets identified for the IM software are protected.

- \*\*C4\*\* lists out all critical assets pertinent to the IM system.

- \*\*S2\*\* outlines the strategy to treat each critical asset separately for arguments ensuring protection.

- \*\*J2\*\* provides a basis for arguing for each asset separately due to clear relationships among them.

- \*\*G3\*\* states that every individual asset is protected.

- \*\*S3\*\* breaks down the argument by types of assets, referencing PEDD classification.

- \*\*C5, J3\*\* under S3 help define types and justify how these belong to the overarching PEDD categories, providing a structured approach to asset protection.

- \*\*G4\*\* is applied multiple times for different types of assets specified in PEDD, asserting the protection status of each type of critical asset.

Each element in the tree is based on a hierarchical structuring principle using GSN, where `SupportedBy` predicates drive the links between goals through strategies, and `IncontextOf` predicates explain the context within which these goals and strategies operate.