To create a security case for an Instant Messaging (IM) software based on the provided security case pattern, we'll replace placeholders (i.e., terms surrounded by `{}`) with relevant terms. The hierarchical tree format will be indicated using dashes to denote different levels.

### Hierarchical Tree Structure for IM Software Security Case

```

Goal(G1, "IM software is acceptably secure in Messaging System")

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

- Context(C2, "Definition and description of Messaging System")

- Context(C3, "Definition of acceptably secure")

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

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

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

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

- Context(C4, "List of IM software critical assets")

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

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

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

- Context(C5, "List of IM software critical asset types in PEDD")

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

- Goal(G4, "IM software critical asset type 1 is protected")

- Goal(G4, "IM software critical asset type 2 is protected")

- Goal(G4, "IM software critical asset type 3 is protected")

- Goal(G4, "IM software critical asset type 4 is protected")

```

### Explanation:

1. \*\*G1:\*\* Initial goal stating that the IM software is acceptably secure within the Messaging System.

- \*\*Contexts:\*\* C1 (Definition of IM software), C2 (Definition of Messaging System), C3 (Definition of acceptably secure).

2. \*\*S1:\*\* Strategy arguing that IM software assets are under protection.

- \*\*Justification:\*\* J1 (Protection of IM software assets supports the security claim).

- \*\*G2:\*\* Derived goal stating that all identified IM software critical assets are protected.

3. \*\*S2:\*\* Strategy providing arguments for each IM software critical asset.

- \*\*Context:\*\* C4 (List of IM software critical assets).

- \*\*Justification:\*\* J2 (Clear relationship between assets).

- \*\*G3:\*\* Derived goal stating that IM software critical assets are protected.

4. \*\*S3:\*\* Strategy arguing based on the type each IM software critical asset belongs to.

- \*\*Context:\*\* C5 (List of IM software critical asset types in PEDD).

- \*\*Justification:\*\* J3 (Types of IM software assets conform to PEDD).

- \*\*G4:\*\* Derived goal for each of the protected critical asset types.

- Four instances of G4, each for a different critical asset type as implied by the multiplicity relationship.

### Placeholder Replacements:

- `{software}` -> IM software

- `{system}` -> Messaging System

- `{acceptably secure}` -> acceptably secure

- `{type}` -> Type (general term replaced in context)

By following this structure and replacing the placeholders appropriately, we generate a consistent and coherent security case for the IM software based on the given pattern.