Based on the provided predicates and replacing the placeholders with the details specific to Instant Messaging (IM) software, here is the structured representation of the assurance case for the security of IM software:

```

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 IM software assets are under protection)

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

|- Goal (G2, All identified IM 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 IM software critical assets)

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

|- Goal (G3, IM software critical asset is protected) [Multiplicity across assets]

|- Strategy (S3, Argument of the type which the IM 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, IM software critical asset which belongs to type Data Storage is protected)

|- Goal (G4, IM software critical asset which belongs to type Process is protected)

|- Goal (G4, IM software critical asset which belongs to type Environment Entity is protected)

|- Goal (G4, IM software critical asset which belongs to type Data Exchange is protected) [Multiplicity for each type]

```

Explanation:

- \*\*G1\*\* represents the top-level goal, claiming that the IM software is secure in an operational environment. Contexts \*\*C1, C2,\*\* and \*\*C3\*\* define the software, the environment, and the meaning of security, respectively.

- \*\*S1\*\* is the strategy explaining how the protection of assets supports the primary goal, backed by \*\*J1\*\*.

- \*\*G2\*\* narrows this to all individual assets listed in \*\*C4\*\*, with \*\*S2\*\* further devising independent arguments for each asset, refined by \*\*G3\*\*.

- \*\*S3\*\* develops arguments based on the type of asset (as categorized by PEDD), specified within the \*\*C5\*\* context and \*\*J3\*\* justification.

- \*\*G4\*\* instances are repeated for each type in the PEDD classification to argue for their protection, enumerated across the typical critical assets listed in \*\*C4\*\*. These diversify the assurance case to address specifics of asset protection as needed by their type from PEDD.

This structured format deeply nests the IM's necessary security claim specifications, laying out a comprehensive assurance argument using GSN. Each component of the security case is contextualized, justified, and specified to reflect the domain and overall security requirements of IM software.