Based on the given predicate rules for the security case pattern and applying them to develop a concrete assurance case for Instant Messaging (IM) software using GSN, the hierarchical tree structure for the Instant Messaging security case can be represented as follows. Specific elements from the pattern have been instantiated with the details relevant to IM software:

```

G1: IM software is acceptably secure in an enterprise system

- C1: IM software defined as a suite of messaging applications used for corporate communications.

- C2: Enterprise system defined as the network and infrastructure in an organization.

- C3: Acceptably secure defined as meeting all corporate security policies and privacy regulations.

- S1: Argument that software assets are under protection

- J1: Protection of software assets supports that IM software is acceptably secure.

-- G2: All identified IM software critical assets are protected

--- C4: Critical assets list includes user data, authentication credentials, and communication channels.

--- S2: Respective arguments of IM software critical assets

- J2: Relationship between assets is clear and can be argued separately.

--- G3: User data as an IM software critical asset is protected

---- S3: Argument of the type to which the IM software critical asset belongs

----- C5: Asset types in PEDD (Protection, Encryption, Detection, Documentation)

----- J3: Asset types are determined according to corporate security policies.

----- G4: User data, classified under 'protected' in PEDD, is secured

----- G4: Authentication credentials, classified under 'encrypted' in PEDD, is secured

----- G4: Communication channels, classified under 'detection', are monitored

----- G4: Documentation processes, classified under 'documentation', are compliant with privacy regulations

```

In this scenario:

- \*\*G1 - G4\*\* are specific goals, where G1 is the overarching goal of ensuring the IM software’s security is acceptable, and G3 and G4 address the protection of specific types of critical assets.

- \*\*S1 - S3\*\* represent strategies each laying out the approach to argue for the protection of IM software and its assets respectively.

- \*\*C1 - C5\*\* provide necessary contexts explaining the software, system, security definition, critical assets, and asset types.

- \*\*J1 - J3\*\* provide justifications linking the protection of assets to the assertion of software security.

The provided structure ensures that each critical asset and its designated protection category (from the Predicate Execution, Detection, and Documentation model) is specifically accounted for, aligning with security strategies and affirming the overall argument for the IM software's security within an enterprise context.