Based on the predicates and domain information provided, let's instantiate the placeholders and expand the security case pattern with specific details about Instant Messaging (IM) software. Below is the hierarchical tree representation of the assurance case.

```

- Goal (G1, "Instant Messaging software is acceptably secure in operational environment")

- In context of:

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

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

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

- Supported by:

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

- In context of:

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

- Supported by:

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

- In context of:

- Context (C4, "List of Instant Messaging software critical assets: Registration information, Registration process, User account information, Authentication information, Login process, Chat logs.")

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

- Supported by:

- Strategy (S2, "Respective arguments for Instant Messaging software critical assets")

- Supported by:

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

- In context of:

- 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")

- Supported by:

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

- Supported by:

- Goal (G4, "Each type-based Instant Messaging software critical asset is protected")

```

This structure reflects a security case for the Instant Messaging software where the main goal (G1) is about ensuring the software's security in an operational environment. Context definitions are provided to clarify key aspects like the software, the environment, and what "acceptably secure" means. The hierarchy progresses to detail the protection of software assets, further breaking down the argument to handle different asset categories as defined in the PEDD classification.

This arrangement not only offers a structured way to understand the security of Instant Messaging software but also emphasizes the essential aspects such as asset clarification and the significance of type-based protection within the broader assurance framework.