Using the pattern provided, I'll instantiate a security case for the Instant Messaging (IM) software. This instantiation will replace placeholders with specific details related to the IM software domain.

\*\*Instant Messaging Security Case Hierarchy\*\*

```

G1: Instant messaging software is acceptably secure in its operational environment.

- C1: Definition and description of Instant Messaging software.

- C2: Definition and description of operational environment.

- C3: Definition of what is considered acceptably secure for Instant Messaging software.

- S1: Argument that Instant Messaging software assets are under protection.

- J1: Protection of Instant Messaging software assets supports that the software is acceptably secure.

- G2: All identified Instant Messaging software critical assets are protected.

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

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

- S2: Respective arguments of Instant Messaging software critical assets protection.

- G3: Each critical asset of Instant Messaging software is protected.

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

- C5: List of software critical asset types in PEDD includes Process, Data Storage, Environment Entity, Data Exchange.

- J3: Types of Instant Messaging software assets are appropriately classified according to PEDD.

- G4.0: Registration information, which belongs to Data Exchange, is protected.

- G4.1: User account information, which belongs to Data Storage, is protected.

- G4.2: Authentication information, which belongs to Data Storage, is protected.

- G4.3: Login process, which belongs to Process, is protected.

- G4.4: Chat logs, which belong to Data Storage, is protected.

```

In this hierarchy:

- \*\*G1, C1, C2, C3\*\* are directly linked to the instantiation of the software as a whole, defining what "secure" means for it.

- \*\*S1\*\* is the primary strategy, supported by justification (J1) that protecting assets secures the software.

- \*\*G2\*\* underlies the critical step of ensuring all identified critical assets are protected, along with the contexts (C4) and justifications (J2) explaining the asset significance and relationship.

- \*\*S2\*\* provides a way to specifically address each critical asset, highlighted more granularly through G3.

- \*\*S3\*\* divides the argument further by asset types (C5), with J3 clarifying their PEDD classifications.

- \*\*G4.X\*\* are detailed goals instantiated for each critical asset classified under PEDD as mentioned in the domain information. Each of these goals shows the completed logical path of protecting every critical asset corresponding to its type.