Based on the predicates given below for a security case pattern, use this pattern to create a security case for Instant messaging (IM) software and display in a hierarchical tree format using dashes (-) to denote different levels.

Goal (G1, {software} is (acceptably secure) in {system})

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

Goal (G3, {software critical asset} is protected)

Goal (G4, {software critical asset} which belongs to {type} is protected)

Strategy (S1, Argument of that software assets are under protection)

Strategy (S2, Respective arguments of software critical assets)

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

Context (C1, Definition and description of {software})

Context (C2, Definition and description of {system})

Context (C3, Definition of {acceptably secure})

Context (C4, List of {software} critical assets)

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

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

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

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

SupportedBy (G1, S1, 1)

SupportedBy (S1, G2, 2)

SupportedBy (G2, S2, 3)

SupportedBy (S2, G3, 4)

SupportedBy (G3, S3, 5)

SupportedBy (S3, G4, 6)

IncontextOf (G1, [C1, C2, C3], 1)

IncontextOf (S1, [J1], 2)

IncontextOf (S2, [C4, J2], 4)

IncontextOf (S3, [C5, J3], 6)

HasPlaceholder (G1)

HasPlaceholder (C1)

HasPlaceholder (C2)

HasPlaceholder (C3)

HasPlaceholder (C4)

HasPlaceholder (G3)

HasPlaceholder (G4)

HasMultiplicity (S2, G4, number of software critical asset = 4)