### Instantiated Safety Case for a Generic Patient-Controlled Analgesia (GPCA) System

\*\*Top-Level Goal:\*\*

- G1: Operational safety is verified in the GPCA system.

\*\*Strategy:\*\*

- S1: Argument over the satisfaction of all specs over GPCA system. (Undeveloped)

\*\*Context:\*\*

- C1: All specs are given by the set of all instances derived from the GPCA specifications.

\*\*Goal:\*\*

- G2: All operational hazards in the GPCA system are mitigated.

\*\*Strategy:\*\*

- S3: Argument over operational hazards in GPCA.

\*\*Context:\*\*

- C2: Operational hazards are identified from the comprehensive hazard analysis document.

\*\*Multiplicity of Goals (For each identified hazard):\*\*

- G3: Specific operational hazard X is mitigated.

- S4: Argument over the applied scenarios of operational hazard X.

\*\*Context:\*\*

- C3: All related scenarios are identified from hazard-specific situation analyses.

\*\*Multiplicity of Goals (For each scenario):\*\*

- G4: Hazard X is mitigated under scenario Y.

\*\*Strategy:\*\*

- S5: Argument over all specifications related to scenario Y.

\*\*Context:\*\*

- C4: All related specifications derived from scenario Y's requirements.

\*\*Multiplicity of Goals (For each specification):\*\*

- G5: Specification Z is appropriate for scenario Y.

\*\*Strategy:\*\*

- S6: Argument the appropriateness of specification Z over properties.

\*\*Context:\*\*

- C5: Properties are defined as all attributes covered by specification Z.

\*\*Multiplicity of Goals (For each property):\*\*

- G6: Property A is appropriate for specification Z.

\*\*Strategy:\*\*

- S7: Argument over the source of the property definition.

\*\*Context:\*\*

- C6: Source is derived from the authoritative database for property A.

\*\*Goals:\*\*

- G7: Source B is appropriate and trustworthy.

- G8: Property A definition is sufficient.

\*\*Solutions (Evidence):\*\*

- Sn1: Verification report based on sources for property A.

- Sn2: Validation report confirming sufficiency of the property A definition.

### Hierarchical Tree Representation

- G1: Operational safety is verified in the GPCA system.

- S1: Argument over the satisfaction of all specs over GPCA system. (Undeveloped)

- C1: All specs are given by the set of all instances derived from the GPCA specifications.

- G2: All operational hazards in the GPCA system are mitigated.

- S3: Argument over operational hazards in GPCA.

- C2: Operational hazards are identified from the comprehensive hazard analysis document.

- G3: Specific operational hazard X is mitigated.

- S4: Argument over the applied scenarios of operational hazard X.

- C3: All related scenarios are identified from hazard-specific situation analyses.

- G4: Hazard X is mitigated under scenario Y.

- S5: Argument over all specifications related to scenario Y.

- C4: All related specifications derived from scenario Y's requirements.

- G5: Specification Z is appropriate for scenario Y.

- S6: Argument the appropriateness of specification Z over properties.

- C5: Properties are defined as all attributes covered by specification Z.

- G6: Property A is appropriate for specification Z.

- S7: Argument over the source of the property definition.

- C6: Source is derived from the authoritative database for property A.

- G7: Source B is appropriate and trustworthy.

- Sn1: Verification report based on sources for property A.

- G8: Property A definition is sufficient.

- Sn2: Validation report confirming sufficiency of the property A definition.