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

- \*\*G1:\*\* Operational safety is verified in GPCA system

- \*\*S1:\*\* Argument over the satisfaction of all specs over GPCA system

- \*\*C1:\*\* All specs are given by spec.allInstances()

- \*\*G2:\*\* All operational hazards are mitigated

- \*\*S3:\*\* Argument over operational hazards

- \*\*C2:\*\* Operational hazards are given by operational hazard.allInstances()

- \*\*G3:\*\* Overinfusion is mitigated

- \*\*S4:\*\* Argument over the applied scenarios of Overinfusion

- \*\*C3:\*\* All related scenarios are given by Overinfusion

- \*\*G4:\*\* Overinfusion is mitigated under scenario (Flow rate does not match the programmed rate)

- \*\*S5:\*\* Argument over all specs related to scenario (Flow rate does not match the programmed rate)

- \*\*C4:\*\* All related specs are given by scenario.Flow rate does not match the programmed rate.spec.allinstances()

- \*\*G5:\*\* spec (SR1.1) is appropriate for scenario (Flow rate does not match the programmed rate)

- \*\*S6:\*\* Argument the appropriateness of spec (SR1.1) over properties

- \*\*C5:\*\* Properties are given by spec.property.allinstances()

- \*\*G6:\*\* Flow rate sensor is appropriate for SR1.1

- \*\*S7:\*\* Argument over the source of the Flow rate sensor definition

- \*\*C6:\*\* Source is given by property.source

- \*\*G7:\*\* FDA standard is appropriate and trustworthy

- \*\*Sn1:\*\* FDA standard

- \*\*G8:\*\* Flow rate sensor definition is sufficient

- \*\*Sn2:\*\* Flow rate sensor

- \*\*G4:\*\* Overinfusion is mitigated under scenario (Dose limit exceeded due to excessive bolus requests)

- \*\*S5:\*\* Argument over all specs related to scenario (Dose limit exceeded due to excessive bolus requests)

- \*\*C4:\*\* All related specs are given by scenario.Dose limit exceeded due to excessive bolus requests.spec.allinstances()

- \*\*G5:\*\* spec (SR1.4) is appropriate for scenario (Dose limit exceeded due to excessive bolus requests)

- \*\*S6:\*\* Argument the appropriateness of spec (SR1.4) over properties

- \*\*C5:\*\* Properties are given by spec.property.allinstances()

- \*\*G6:\*\* Trusted software limit is appropriate for SR1.4

- \*\*S7:\*\* Argument over the source of the trusted software limit definition

- \*\*C6:\*\* Source is given by property.source

- \*\*G7:\*\* Expertise opinion is appropriate and trustworthy

- \*\*Sn1:\*\* Expertise opinion

- \*\*G8:\*\* Trusted software limit definition is sufficient

- \*\*Sn2:\*\* Trusted software limit

- \*\*G3:\*\* Underinfusion is mitigated

- \*\*S4:\*\* Argument over the applied scenarios of Underinfusion

- \*\*C3:\*\* All related scenarios are given by Underinfusion

- \*\*G4:\*\* Underinfusion is mitigated under scenario (Programmed rate too low)

- \*\*S5:\*\* Argument over all specs related to scenario (Programmed rate too low)

- \*\*C4:\*\* All related specs are given by scenario.Programmed rate too low.spec.allinstances()

- \*\*G5:\*\* spec (SR1.2) is appropriate for scenario (Programmed rate too low)

- \*\*S6:\*\* Argument the appropriateness of spec (SR1.2) over properties

- \*\*C5:\*\* Properties are given by spec.property.allinstances()

- \*\*G6:\*\* 15-minute period trigger is appropriate for SR1.2

- \*\*S7:\*\* Argument over the source of the 15-minute period trigger definition

- \*\*C6:\*\* Source is given by property.source

- \*\*G7:\*\* Previous knowledge is appropriate and trustworthy

- \*\*Sn1:\*\* Previous knowledge

- \*\*G8:\*\* 15-minute period trigger definition is sufficient

- \*\*Sn2:\*\* 15-minute period trigger

- \*\*G4:\*\* Underinfusion is mitigated under scenario (Flow rate is less than 90% of the programmed rate setting)

- \*\*S5:\*\* Argument over all specs related to scenario (Flow rate is less than 90% of the programmed rate setting)

- \*\*C4:\*\* All related specs are given by scenario.Flow rate is less than 90% of the programmed rate setting.spec.allinstances()

- \*\*G5:\*\* spec (SR6.1.3) is appropriate for scenario (Flow rate is less than 90% of the programmed rate setting)

- \*\*S6:\*\* Argument the appropriateness of spec (SR6.1.3) over properties

- \*\*C5:\*\* Properties are given by spec.property.allinstances()

- \*\*G6:\*\* Reliable alarm system is appropriate for SR6.1.3

- \*\*S7:\*\* Argument over the source of the reliable alarm system definition

- \*\*C6:\*\* Source is given by property.source

- \*\*G7:\*\* Previous knowledge is appropriate and trustworthy

- \*\*Sn1:\*\* Previous knowledge

- \*\*G8:\*\* Reliable alarm system definition is sufficient

- \*\*Sn2:\*\* Reliable alarm system

- \*\*S2:\*\* Argument over reliability in all suitable levels of GPCA system (Undeveloped)

Each level deeper in the hierarchy is represented by a higher indentation with dashes, indicating the structure of the safety case.