Below is the instantiated security case for ACAS Xu (Airborne Collision Avoidance System Xu) derived from the given security case pattern:

```

G0: ACAS Xu satisfies security requirements

- S0: Argue through asset protection and secure development requirements

- G1: ACAS Xu satisfies the asset protection requirements

- A1: Asset inventory is established

- S1: Argue through the different stages of the system development life cycle

- G3: Asset protection requirements are met during the architecture design phase

- C2: Description of ACAS Xu architecture

- S2: Argue through derivating security threats from SRs

- J1: Detection and mitigation of threats fulfill SRs

- G5: ACAS Xu architecture is protected against identified security threats (STs)

- A2: All relevant threats have been identified

- S3: Argue over each security threat

- G0.1: ACAS Xu architecture is protected against ST1 (Tampering)

- G0.2: ACAS Xu architecture is protected against ST2 (Spoofing)

- G0.3: ACAS Xu architecture is protected against ST3 (Elevation of privileges)

- G6: ACAS Xu architecture is validated

- C3: Description of ACAS Xu architecture model

- A3: ACAS Xu architecture model is well defined in formal method (e.g., UML)

- G4: Asset protection requirements are met during other phases (undeveloped)

- G2: ACAS Xu satisfies secure development requirements (undeveloped)

- C0: Description of ACAS Xu

- C1: SR are requirements about protecting the system from malicious entities

- J0: The argumentation is based on satisfaction of SRs

- A0: System SRS are complete, adequate, and consistent

```

### Justification and Explanation

1. \*\*Instantiation and Context:\*\*

- The top-level goal (G0) claims that ACAS Xu satisfies security requirements.

- Supporting context (C0) describes ACAS Xu.

- C1 provides information that SRs (security requirements) are about protecting the system from malicious entities.

- J0 and A0 justify that the arguments are based on the satisfaction of SRs, and assume that requirements are complete and consistent.

2. \*\*Asset Protection Requirements:\*\*

- G1 captures that ACAS Xu satisfies asset protection requirements.

- The context C2 describes the architecture of the system, i.e., ACAS Xu.

- The decomposition is captured through S1, which argues by stages of development:

- G3 focuses on the architectural design phase (important for defining initial security measures and validating security design).

- C2 and J1 are used to denote the reliance on security threat identification from security requirements.

- G5 deals with protection against specific identified threats.

- Decomposition through S3 leads to specific security threats G0.1, G0.2, and G0.3 derived from the domain threats.

3. \*\*Validation:\*\*

- G6 is dedicated to validating the system’s architecture, supported by context C3 and assumption A3.

4. \*\*Handling Specific Threats:\*\*

- Specific goals G0.1, G0.2, and G0.3:

- These threats (ST1, ST2, ST3) are carried over from the domain information provided, converting the threats into specific protection goals within the secure system's context.

5. \*\*Secure Development Process:\*\*

- G2 captures that ACAS Xu satisfies secure development requirements, although in this implementation, it’s noted as undeveloped.

6. \*\*Remaining Undeveloped Sections:\*\*

- G4 denotes asset protection must also be verified in phases other than architectural.

- These sections are labeled “undeveloped” as some arguments need further expansion specifically suitable to ACAS Xu’s lifecycle.

Each item within the hierarchical structure ensures that all generic placeholders from the initial pattern are replaced with specific information about ACAS Xu, making this a concrete security case.