Based on the security case pattern provided for the ACAS Xu (Airborne Collision Avoidance System Xu), and by replacing placeholders with specific information, here is the instantiated security case in a hierarchical tree format using GSN elements:

```

G0: ACAS Xu satisfies security requirements

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

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 the ACAS Xu architecture

S2: Argue through deriving security threats from SRs

J1: Detection and mitigation of threats fulfill SRs

G5: ACAS Xu architecture is protected against identified security threats

A2: All relevant threats have been identified

S3: Argue over each security threat

G0.X: ACAS Xu architecture is protected against [specific threat, e.g., unauthorized access]

G6: ACAS Xu architecture is validated (undeveloped)

C3: Description of ACAS Xu architecture model

A3: ACAS Xu architecture model is well defined in [formal method] (uninstantiated)

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

G2: ACAS Xu satisfies secure development requirements (undeveloped and uninstantiated)

```

The GSN tree visually represents the security case with goals (G), strategies (S), contexts (C), assumptions (A), and justifications (J). It is assumed that an actual formal method for A3 and specific threats for G0.X would be further detailed in a complete security case instantiation.