Based on the given predicates for a security case pattern for threat identification, here is the instantiated security case for ACAS Xu, represented in a hierarchical tree format:

```

- 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 architecture

- S2: Argue through derivating security threats from 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.X: ACAS Xu architecture is protected against STX

- G6: ACAS Xu architecture is validated

- C3: Description of ACAS Xu architecture model

- A3: ACAS Xu architecture model is well defined in formal method

- J1: Detection and mitigation of threats fulfill SRs

- G4: Asset protection requirements are met during other phases

- G2: ACAS Xu satisfies secure development requirements

```

This hierarchical tree follows the process of instantiating the assurance case pattern by replacing placeholders with system-specific information about ACAS Xu and structuring the elements and their relationships as defined by the predicates. Some goals such as G4 and solutions such G2, G6, and G0.X remain undeveloped or require further development, reflected by their decorators.