Based on the provided security case pattern and the domain information about ACAS Xu, the instantiated security case for ACAS Xu is structured as follows:

```

G0: "ACAS Xu satisfies security requirements"

- C0: "ACAS Xu"

- C1: "Security Requirements (SRs) are requirements about protecting the system from malicious entities"

- J0: "The argumentation is based on satisfaction of SRs"

- A0: "ACAS Xu 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 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"

-------- G0.1: "ACAS Xu architecture is protected against ST1"

-------- G0.2: "ACAS Xu architecture is protected against ST2"

-------- G0.3: "ACAS Xu architecture is protected against ST3"

------ G6: "ACAS Xu architecture is validated" (Uninstantiated and Undeveloped)

------- C3: "Description of ACAS Xu architecture model" (Uninstantiated)

------- A3: "ACAS Xu architecture model is well defined in formal methods framework" (Uninstantiated)

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

-- G2: "ACAS Xu satisfies secure development requirements" (Uninstantiated and Undeveloped)

```

This hierarchy visually represents the expanded version of the GSN patterns with specific details for the ACAS Xu system. Uninstantiated and undeveloped elements are noted, indicating areas where more specific information or development is necessary. Assumptions, contexts, and justifications provide additional reasoning to support the goals, aligning them directly with the system's security needs. Each goal G0.X instantiated per identified security threat reflects how the system's architecture secures against these specific threats (ST1, ST2, ST3).