Creating a security case for ACAS Xu (Airborne Collision Avoidance System Xu) using Goal Structuring Notation (GSN) involves establishing the top-level safety goal, breaking it down into sub-goals, and providing rationale, assumptions, context, and evidence for each part. Below is an example formatted as an hierarchical tree using dashes to denote different levels.

```plaintext

- G1: ACAS Xu is secure from unauthorized access and manipulation.

- S1: System-level security policies and procedures are implemented.

- C1: Context of the organization's security policies.

- A1: Assumption that organizational security policies are up-to-date.

- E1: Evidence: Review of organizational security policy documentation.

- G2: Data communication in ACAS Xu is secure.

- S2: All communication channels are encrypted.

- C2: Context of communication protocols used.

- A2: Assumption that encryption standards are adhered to.

- E2: Evidence: Encryption protocol certification.

- S3: Integrity checks are performed on all data transfers.

- C3: Context of data integrity mechanisms.

- A3: Assumption that integrity-check algorithms are robust.

- E3: Evidence: Logs showing successful integrity checks.

- G3: Physical security of ACAS Xu components is ensured.

- S4: ACAS Xu hardware is protected against physical tampering.

- C4: Context of physical security measures employed.

- A4: Assumption that physical security standards are maintained.

- E4: Evidence: Audit of physical security controls.

- S5: Access to ACAS Xu hardware is controlled and monitored.

- C5: Context of access control mechanisms.

- A5: Assumption that access control policies are enforced.

- E5: Evidence: Access logs and security cameras footage.

- G4: ACAS Xu software is secure from vulnerabilities.

- S6: All software components undergo regular security assessments.

- C6: Context of security assessment procedures.

- A6: Assumption that security assessments are comprehensive.

- E6: Evidence: Reports from recent security assessments.

- S7: Secure coding practices are followed in the development of ACAS Xu software.

- C7: Context of secure coding standards.

- A7: Assumption that all developers are trained in secure coding.

- E7: Evidence: Code review records and developer training certificates.

- G5: ACAS Xu is resilient to cyber-attacks.

- S8: Incident response plans are in place and regularly tested.

- C8: Context of incident response plans.

- A8: Assumption that incident response plans cover all scenarios.

- E8: Evidence: Results from recent incident response drills.

- S9: Continuous monitoring for potential cyber threats is in place.

- C9: Context of monitoring tools and strategies.

- A9: Assumption that monitoring systems are effective.

- E9: Evidence: Logs from monitoring systems showing detection of potential threats.

```

In this structure:

- Goals (G) define the key security objectives.

- Strategies (S) explain how the goals are going to be achieved.

- Contexts (C) provide relevant background information.

- Assumptions (A) list the assumptions made during the security case development.

- Evidence (E) provides the proof that the strategies and assumptions are valid.

This hierarchical structure showcases a thorough breakdown of security aspects for ACAS Xu.