To create a security assurance case for ACAS Xu (Airborne Collision Avoidance System Xu), we will utilize the Goal Structuring Notation (GSN). Below, the goal structures are displayed in a simple hierarchical tree format. Each main goal (G) is supported by strategies (S), which are further supported by sub-goals, assumptions (A), justifications (J), and solutions (Sn) as applicable.

### ACAS Xu Security Assurance Case

1. \*\*G1: Ensure that ACAS Xu system is secure against unauthorized access\*\*

- S1: Implement and validate secure access controls

- G1.1: Implement robust authentication mechanisms

- Sn1.1: Use of multi-factor authentication systems

- A1.1: Users are assigned unique credentials

- G1.2: Implement rigorous authorization practices

- Sn1.2: Role-based access control systems in place

- J1.2: Access levels are defined according to job responsibilities

2. \*\*G2: Guarantee the integrity of ACAS Xu operational software\*\*

- S2: Employ secure software development lifecycle (SDLC) practices

- G2.1: Use code signing to ensure software integrity

- Sn2.1: Implementation of digital signatures and secure key storage

- G2.2: Conduct regular security audits of the software

- Sn2.2: Regular audits by internal and external security experts

- J2.2: Previous audits have identified vulnerabilities timely

3. \*\*G3: Maintain the confidentiality of ACAS Xu communication and data\*\*

- S3: Implement effective encryption methods

- G3.1: Encrypt sensitive data in transit and at rest

- Sn3.1: Use of AES-256 encryption for data protection

- A3.1: Data encryption keys are managed securely

- G3.2: Establish secure communication channels

- Sn3.2: Use of VPN tunnels for remote communications

- J3.2: VPNs mitigate the risk of data interception

4. \*\*G4: Ensure the availability of ACAS Xu during operations\*\*

- S4: Design for fault tolerance and redundancy

- G4.1: Implement redundant systems and components

- Sn4.1: Duplication of critical system components

- J4.1: Redundancy ensures continuity during component failures

- G4.2: Regular system maintenance and updates

- Sn4.2: Scheduled maintenance and patch management procedures

- A4.2: Maintenance conducted by trained personnel

5. \*\*G5: Ensure the ACAS Xu system is resilient against cyber-attacks\*\*

- S5: Integrate continuous monitoring and incident response

- G5.1: Deploy intrusion detection systems (IDS)

- Sn5.1: Implementation of network-based and host-based IDS

- G5.2: Establish a rapid incident response team

- Sn5.2: Procedures and protocols for the incident response team

- A5.2: The response team is available 24/7

This tree structure shows how each main goal of the ACAS Xu security case is supported by specific strategies, assumptions, justifications, and evidence, building a comprehensive case for the system’s security.