7. Zero Trust Avionics Systems

https://www.researchgate.net/publication/374554536_Zero_Trust_Avionics_Systems_ZTAS

Zero Trust Avionics Systems (ZTAS). (2023, October 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10311248

1. **Challenges in Avionics System Security**: Designing the next generation of avionics systems for aircraft and spacecraft platforms poses significant challenges, especially in terms of cybersecurity, given the sensitivity of electronic equipment onboard.
2. **Vulnerability to Cyber Attacks**: The networked architecture of avionics systems makes them susceptible to cyber-attacks and intrusions, which can have catastrophic effects on safety-critical systems by influencing physical processes and flight dynamics through digital manipulations.
3. **Need for Zero Trust Avionics Systems (ZTAS)**: To mitigate risks of cyber-attacks and intrusions in safety-critical flight control systems, there is an essential need for implementing Zero Trust Avionics Systems (ZTAS) based on the Zero Trust architecture (ZTA) principle.
4. **Principles of Zero Trust Architecture**: The ZTA operates on the principle of “never trust, always verify,” eliminating the concept of trust from avionics systems architecture. This approach is vital for protecting modern digital and embedded systems in flying vehicles.
5. **Integration of Cybersecurity in Avionics Systems**: Seamless integration of cybersecurity features within avionics systems is crucial, ensuring that added Zero Trust security components do not impede the functionality of avionics systems.
6. **Designing Functionality and Zero Trust Security Simultaneously**: There is a need for well-defined approaches to design functionality and Zero Trust cybersecurity simultaneously for avionics systems, ensuring system confidentiality/security, integrity, and maintaining functionality.
7. **Guiding Principles for ZTAS Design**: The paper proposes four guiding principles for designing ZTAS - Never trust, always verify; Assume breach; Verify each action explicitly; and Apply unified analytics. These principles will be used to translate Zero Trust principles for ZTAS design, providing a preliminary framework for ZTAS development.

These key points emphasize the importance of incorporating advanced cybersecurity measures like Zero Trust in avionics systems to address the evolving nature of cyber threats and ensure the resilience and security of avionics systems in aircraft and spacecraft platforms.