

Thoughts on ADS-B in light of security concerns

In light of the aftermath of the events of 9/11/01, I expect the security aspects of ADS-B to come under the magnifying glass. Certainly a number of issues were raised in the past discussions when developing the ADS-B MASPS, but now we may have to face up to issues. The following list is just food for thought for WG6.

1. In re-opening the NAS for private aircraft the DoD secretary indicated that all aircraft would be required to file flight plans and to be under ATC control. It is not clear if this is just a temporary measure or represents a new reality for the way GA will have to operate in the future NAS. If the latter, the idea of anonymity will no longer exist in the NAS, nor will need to be supported by ADS-B.

2. Probably the most fundamental security issue with ADS-B is the core idea of broadcasting the identity and precise location of each aircraft. This would open the door for a terrorist to attack specific aircraft or aircraft of a specific airline or corporation. While some people have suggested some form of encryption might be applied, I do not see any way in which this could be effective without fully undermining the basic ADS-B concept and associated benefits. A closed community, such as DoD or a given airline, could perhaps apply an effective cryptographic technique to limit to that community those can successfully receive and decode ADS-B messages. However, I do not foresee any viable scheme that would accommodate such basic applications as CDTI on a NAS-wide basis and at the same time prevent a terrorist from successfully receiving ADS-B information. I'm not saying this is a show-stopper for ADS-B. Rather, I just believe that WG6 and SC-186 will need to consider this most fundamental of security issues raised by ADS-B. I would also note that a few years ago IFALPA raised this as an issue for ADS in general.

3. As already briefly noted in DO-242 some applications may require independent validation of the ADS-B information. This has two aspects. One is simply to detect failures that result in errors in the reported aircraft location. The second is to detect spoofing and this is the aspect where the security concerns are raised.

4. Since the 9/11/01 events the vulnerability of GPS to a denial of service attack has come under a lot of attention. While DO-242 addresses a secondary source of navigation data, perhaps DO-242A needs to make it clear that certain safety applications can only be supported if a suitable independent source of navigation data is available (perhaps for both the transmitting and the receiving aircraft).