NEASCOG CNS Security Statement

Security is a relatively new concept for aviation. In general terms, it could be said that aviation has traditionally been based on open trust as a peaceful commercial activity. 'Classical' hijacks followed by bombing of aircraft in flight and 9/11 attacks were in the past the security concerns for aviation. Subsequent to 9/11 there have been other forms of attack on aviation involving MANPADs[1], laser illumination (against pilots and tower controllers) and bombing of airport land side.

Current threat and risk assessments consider the risk of 'electromagnetic attack' on CNS systems as medium (jamming) to low (spoofing, unlawful exploitation). However, the same assessment indicates that further work is needed to understand the types and likelihood of attacks and their criticality and impact. A continual pro-active threat evolution watch is required to permanently adapt the security system to cope with the ever changing landscape of actual threats and risks.

ATM is moving to a net centric operational environment, becoming more dependent on cyber and digital technological enablers. This brings important advantages, but also introduces new threats and risks, and stronger interdependencies with safety, capacity, crisis management and critical infrastructure protection. Common policies and strategies are required.

Organisations like ICAO, the FAA, NATO, ECAC, EUROCONTROL and the aeronautical industry are engaged in continual assessments to identify threats, vulnerabilities, and risks to the ATM system and to keep mitigation measures current. The ANSPs have an important role in identifying the ATM/CNS system security architecture, and industry stands ready to support. The approach is a security model 'intelligence-driven, threat based and risk managed'.

Legacy CNS technologies have been developed with little or no security built-in by design, and new CNS technologies are now giving full consideration to cyber security requirements. The design process must move from safety considerations to safety and security considerations. It means that, like for cyber security, a security layer needs to be added on top of a 'non-secure by design system'. Future development must have a different approach. The threat assessment process includes identification of threats and vulnerabilities, evaluation of the resulting operational impact, and development of all potential mitigations, which then leads to development of ground and airborne requirements that feed the design process. The security design must be considered for the overall life cycle: conceptual, design, prototype, development, deployment, operation and decommission. Development of cyber security standards is key to this process.

At present, some CNS systems upgrades are under study or are being implemented to reduce the risk of spoofing, interference, jamming and unlawful exploitation of signals. Besides this, for the short and medium term, the best security measure is ground system **redundancy**. This may include a multi-link concept for future communication infrastructure (FCI), multi-constellation (GNSS) for navigation and multiple layer coverage (radar/WAM[2]/ADS-B) for ground surveillance.

[1] Man-portable air-defence system
[2] Wide Are Multi-Lateration

For the longer term, it is expected that technical security features will be naturally embedded into future system configurations (e.g. IP security).

Pro-active security management at national and international levels is leading to a comprehensive holistic approach to ATM security, which includes looking into the overall spectrum of threats and identifying affordable implementation strategies for risk mitigation and reduction to acceptable or tolerable levels. Collaborative sharing of threat information reduces risk on all sides. This risk management process is a continual exercise allowing the ATM system to quickly adapt to evolving and changing threats.