**WPosition Paper on Aircraft Penetration Testing**

Aircraft and supporting ground systems rely on properly configured information technology systems and secure software. Hard- and software is modified, updates are installed and new functions may be introduced many times during the lifecycle of an aircraft. This is done either directly into the systems within the aircraft or into the ground systems. These systems may consist of so-called “commercial off the shelf” (COTS) products. Vulnerabilities for COTS systems are often publicly documented but patches are usually not provided or not provided in a timely manner by OEMs for COTS-based components in aircraft and ground systems. Furthermore, aircraft rely on more network-based interconnection of components and are equipped with broadband connectivity for air to ground communication including internet connectivity for operational and passenger use (e.g., passenger WiFi). Especially aircraft of newer generations have reduced segregation of systems and increased network-based interconnection. As development of such systems and software is complex, even carefully designed and implemented products potentially have vulnerabilities not being detected during development and production. During the lifecycle of a product new threats and attack vectors may arise that have not been considered previously.

A common and proven measure to detect such vulnerabilities is security testing including penetration testing. During penetration testing security experts try to compromise the system in question. They play the role of the cyber criminals but for the good. As aircraft are regulated systems penetration testing faces some challenges such as avoiding any potential side effects and ensuring a reset to its normal operational state after the tests. Otherwise, the aircraft could be out of its specifications and the type certificate may be at risk. However, the overall benefits of security testing (e.g., detecting unknown vulnerabilities and weaknesses) and the resulting assurance provided through the tests are major benefits of conducting such tests. As an operator, we are responsible for the safety and security of our passengers and crews and therefore must take all reasonable measures to protect our aircraft against cyber attacks. Thus, operators must be allowed to conduct security tests on their aircraft while being fully supported by OEMs.

**Proposed Measures for Improvement**

To empower the operator conducting responsible penetration testing on its aircraft, we propose:

- **OEMs have to provide procedures to reset aircraft in a state that is in accordance with its specifications after penetration testing**
  When conducting penetration testing in traditional IT systems, either a testing system that is identical with the production system is used or the production system is backed up before the penetration test, so that it can be reset to the pre-testing state. We request OEMs to support the operators in conducting penetration testing in a similar responsible way and are willing to include the OEMs in all penetration tests we may conduct on aircraft. OEMs should define and support procedures to restore an aircraft’s original state that is in accordance with its type certificate after penetration testing is completed. Assurance over the successful execution of such procedures should be provided, proving all systems are reverted to their original state. Even without conducting penetration tests, such a function is necessary due to the risk of real hacking attempts to our aircraft.

- **Confidential disclosure of security measures and architecture to allow the operator evaluate the cyber security state of its aircraft**
  OEMs design the cyber security protection measures of the aircraft as well as the information technology systems and software. As the operators are finally responsible for the safety and security, he must be equipped with proper documentation about the security architecture, measures implemented and their default secure configuration. Only with such information, appropriate evaluation of the current security state of their aircraft as well as necessary risk management is possible on the operator's side. Thus, it is the OEMs' duty to provide such information in an adequate way and level of detail. The less details OEMs provide the higher the risk of unintended and potentially unknown side effects is. If information is provided, it helps to faster detect and mitigate vulnerabilities and learn for future products. With the continuously growing risk of (successful) cyber-attacks, provisioning of black box systems is not an option for operating secure e-enabled aircraft. Security by obscurity is not an acceptable security measure.

- **Conduct penetration testing during development and during the lifecycle and provide information of the OEMs own testing and results**
  Penetration testing should be conducted during aircraft development as well as during the lifecycle, especially when software updates are released and at least annually. Supervisory bodies may set standards for OEM conducted penetration testing. Furthermore, an independent body should conduct penetration tests. As for all cyber security measures, operators must receive assurance about the tests regarding their scope, conduction and results of the tests. Thus, OEMs should inform the operators about how they tested and what tests they conducted as well as about the outcome of the tests. The results of a penetration test may reveal security shortcomings that are not fixed yet. Operators should have a chance to assess these potential shortcomings and risks that may arise thereof and whether they are within their risk appetite. Sharing such information would also reduce the effort for all operators and the OEMs to conduct similar tests several times. OEMs must commit to provide patches to fix exploitable vulnerabilities in a timely manner depending on the criticality of the findings and according to SLA.
  Of course, penetration testing is only one of many security measures that must be in place and cannot replace but complement other measures such as a secure development lifecycle, regular code reviews, testing and vulnerability scans.

Overall, penetration testing and responsible usage of the results increase the security for everyone and should be in the mutual interest of operators and OEMs alike. **Potential findings would be confidentially shared back to the OEMs** in a cooperative approach to improve the security of their products and in return make our industry even more secure.