ATM & AIRPORT
CYBER SECURITY
MANAGEMENT

Traffic Control Systems

THE ROAD TOWARDS A SECURE ATM SYSTEM

Increased automation, connectivity and reliance on digital information have raised concern over the risks inherent in the interconnected nature of the ATM system of systems. It is crucial that ATM systems ensure data security and continuous operational availability and integrity in a world of ever-changing cyber threats.

Future operational concepts, such as those developed by SESAR and NextGen, will increasingly rely on new technologies, connectivity methods and architectures which entail new vulnerabilities and threats.

Security represents an evolving, ever-changing and persistent challenge to the ATM world and, with the introduction of the Amendment 16th of ICAO ANNEX 17, also a duty for each ATM stakeholder. From November 2018 each ATM Stakeholder will be obliged to develop and implement measures to protect their ATM systems from unlawful interference in accordance with their risk assessment.

To win the security war it is necessary to first recognize that security solutions are part of a wider process. Delivering ATM Security should be seen as an evolving and continuous process completely integrated in the ATM system lifecycle.

Leonardo is on the frontline in the fight for a secure and resilient ATM system with a leading role in research initiatives, such as coordination of the European ATM Security project GAMMA (Global ATM Security Management - www.gamma-project.eu), and strong involvement in international working groups. Leonardo has established the processes, tools and practices to stay ahead of this race, also leveraging on its broad presence in the wider cyber domain. First-hand experience in the development of security solutions within a complex and evolving international regulatory framework provides the foundations for supporting customers with guidance over the implementation of standards and regulations.

ATM & AIRPORT CYBER SECURITY MANAGEMENT

Leonardo methodologies, tools and processes open the way for secure and resilient ATM systems.

- **Why Secure:** the ATM systems can be protected against threats and vulnerabilities and provide security ATM services in support of organizations and authorities engaged in aviation security, national security, defence, and law enforcement.
- **Why Resilient:** the ATM systems can be prepared for disruptions and adapt to changing conditions and to respond and recover rapidly from interferences to ensure the continuity of services at an acceptable performance level.

Secure by design
Information Security Assurance is a fundamental preliminary requirement in any ATM Technological component developed by Leonardo.

Our ATM System Security Management process follows the ISO/IEC 27000 family of standards to deliver secure by design ATM systems. The design methodology starts from the definition of an ATM System Security Management Plan describing the ATM system assets with their interconnections, the security perimeter and the the list of all security activities. The ATM System Security Risk Management represents the core of the design strategy put in place by Leonardo, including the following steps:

- The **system security risk assessment** aims at identifying, analysing and evaluating the security risks affecting the ATM system.
- The **system risk treatment** aims at reducing the medium and high risks by decreasing the risk related to assets and interfaces, acting on the likelihood and/or the consequences through the identification and the definition of security countermeasures.
- The **Implementation of security countermeasures** supporting the customer in defining a set of effective Security Requirements most suited to their needs.

Application of this process provides the foundations for identifying the Security Requirements laying the ground for the definition, design and development of the appropriate Security Solution, easily integrated with existing or new ATM systems.

ATM SECURITY SOLUTIONS

Leonardo has the experience and know-how to deploy a range of technical security solutions adapted and customised to the specific ATM environment and targeting the evolving nature of the cyber attacks, such as data leakage or manipulation, DDoS, unauthorised access, re-routing of messages, malware diffusion, software manipulation, etc.
Our security solutions provide comprehensive protection at network, system and application level, based on a detailed assessment of customer needs.

Some of the most commonly adopted solutions are listed below:

- Access control management for applications, systems and network devices
- User Privilege Management
- Malware Protection
- Secure configuration and Security Hardening
- Secure Software Development
- Boundary Protection (Firewall & IDS/IPS)
- Virtual Private Network (VPN)
- Network Security Management
- Secure Data Transfer
- Alarm and Log Collection, protection and monitoring

- Service and Data availability (back-up, redundancy, Disaster Recovery)
- Vulnerability Management (Security Source Code Analysis, Penetration Testing).

Leonardo ATM systems are flexible and open for easy integration with a Security Operation Center (SoC) or any security tool (e.g. IAM, PIM and SIEM) selected for optimal implementation in the customer's environment.

CYBER SECURITY SOLUTIONS

Intelligence - driven threat mitigation
Leonardo is a global leader in the field of Cyber defence solutions for the protection of Critical National Infrastructures. Our approach includes a wide range of aviation specific cyber security services and solutions which provide an ANSP or airport organisation with an assured security strategy: assessment of the IT and OT estates; risk analysis and management; design, protective monitoring; training and assistance.

Leonardo's combined experience in the development of Air Traffic Management systems and intelligence driven cyber defence programs allows a unique insight into the threats our customers are facing and the solutions that can be deployed to mitigate risks, reducing the potential impact on the essential services that our clients provide.

To this aim we have developed a range of solutions aimed at the following:

- Critical infrastructure access management & monitoring solutions
- Denial of service monitoring and protection
- Endpoint and data Integrity protection services

Cyber consulting services
Leonardo has qualified teams of consultants who have developed a full set of skills including deep technical, regulatory and organisational experiences. Services provided include:

- Security infrastructure assessment, design and review
- Security assessment and audit
- Security Certification support for ISO 27001, ISO 22301 and Common Criteria (providing Leonardo LVS support to comply with National and International Certification Schema)
- Governance, risk and compliance management
- Business continuity & disaster recovery planning
- Information security awareness and training
- Application security/secure coding.

We also offer turnkey solutions based on an analysis of customer needs, comprising architecture and design specification, implementation, and on-site integration. Those include the design of custom SOCs, secure collaboration solutions, information management with a particular focus on document classification and protection, and secure web applications.

- Network and application design & protection
- Endpoint security
- Identity management, PKI and digital signatures
- Cloud security and virtual environment protection
- Malware analysis.

ATM & AIRPORT CYBER SECURITY MANAGEMENT

INTELLIGENT CYBER SECURITY SERVICES

Intelligence & analysis
The Leonardo IOC (Intelligence Operating Centre) provides actionable intelligence based on real time analysis of open information sources; deep and dark web, obtained through data mining, machine learning algorithms and a high performance computing framework integrated with data feeds from select partners and CERTs. Following analysis are available:

- Social network analysis
- Network analysis for intelligence and surveillance
- Security prevention & early warning
- Brand protection - reputation analysis
- Fraud & anti phishing
- Transaction monitoring & alert management
- Data breach response.

Protective monitoring & estate management services
Our cyber security and intelligence services offer efficient, around-the-clock perimeter and internal security with real-time monitoring of both IT and OT infrastructures, device maintenance, event correlation, and analysis of the customer's infrastructure and critical applications to ensure the cyber threat is pro-actively managed and attacks mitigated.

INCIDENT RESPONSE SERVICES

Our incident response services cover the entire spectrum from initial incident and the provision of threat intelligence, to forensic services and advanced malware analysis to establish both nature and origin of the attack:

- Incident response services identify the most appropriate containment and reaction strategy, reducing business impact and supporting remediation
- Threat intelligence services gather information on both existing and emerging threats
- Forensic services collect, store and provides all the evidence typically required for forensics.

CERTIFICATIONS AND STANDARDS

- UNI EN ISO 9001:2008 "Quality management systems – Requirements"
- EN 9100:2016 "QMS – Requirements for Aviation, Space & Defense Organizations"
- ISO/IEC 27001:2013 "Information technology — Security techniques — Information security management systems — Requirements"
- LSR18.6E certified infrastructure (Lampertz room)
- Leonardo LVS (Consorzio RES) accredited to OCSI (Organismo di Certificazione della Sicurezza Informatica)
- NIST Guidelines (sp800-171, sp500-299, Framework for Improving Critical Infrastructure Cybersecurity)
- ISO/IEC 27000 family - Information security management systems.

LEONARDO
SECURITY & INFORMATION SYSTEMS

For more information please email marketing_TCS@leonardocompany.com
Leonardo S.p.a.
Via Tiburtina, Km 12.400 - 00131 Rome - Italy - Tel: +39 06 41501 - Fax: +39 06 4131133