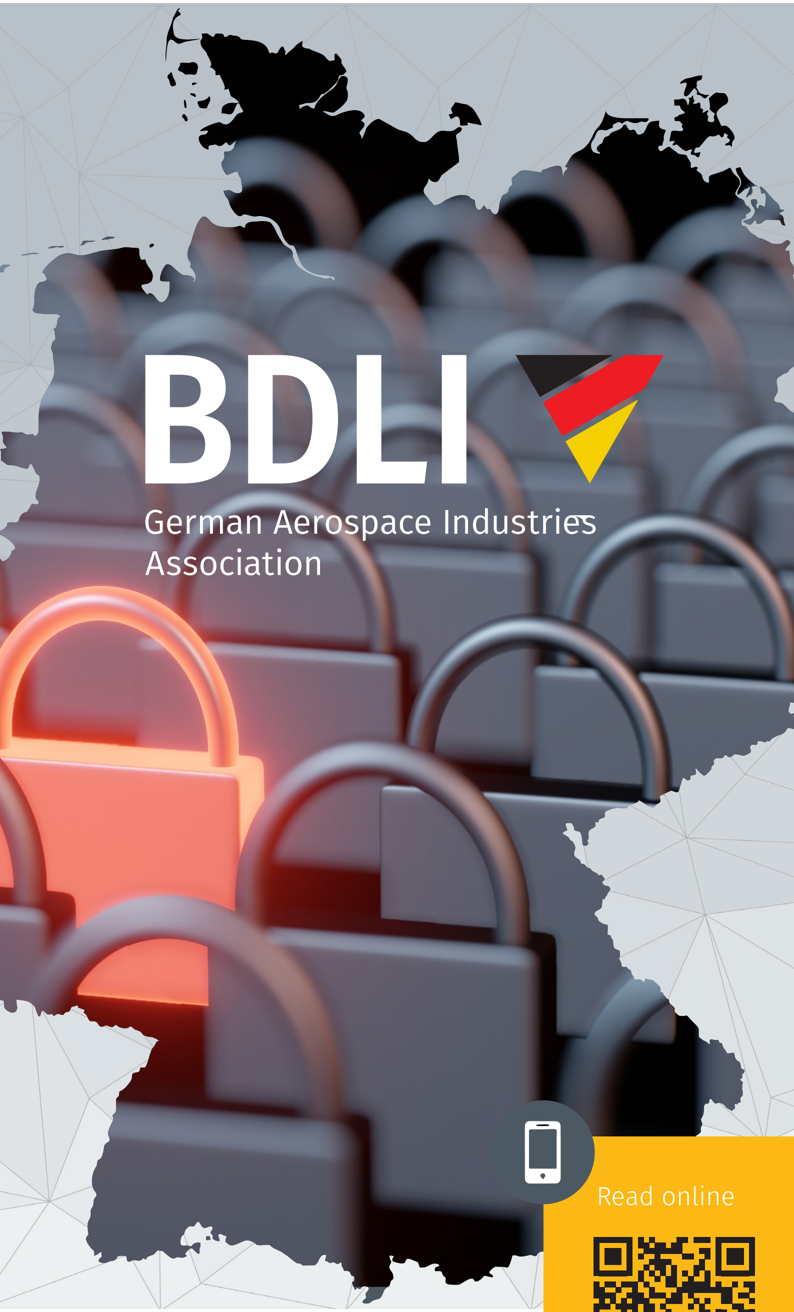
GLOSSARY

1/2020



BDLI

German Aerospace Industries Association

Read online

Published by the BDLI Committee on Cyber Security

Read online

GLOSSARY

Aerospace cyber security threats, measures, best practices and standards are the subject of numerous documents and publications from a wide range of organizations. The multitude of publications, the different perspectives and focal points in the publications lead to a diversity that makes it difficult for interested and affected companies to classify the relevance for themselves and to form priorities in perception and implementation.

With this glossary, the Cyber Security Committee of the BDLI would like to present a meaningful collection of relevant standards in order to facilitate the selection of targeted publications. This compilation does not claim to be exhaustive, but serves as an orientation and approach to the topic of cyber security. For all standards listed here, we have provided URL‘s, outlined the relevant sector and briefly described the objectives and focal points of the standards. This glossary can and should be extended and we are looking forward to receiving your comments by e-mail: friebe@bdli.de

Standard: Doc 8973

Organization: ICAO (International Civil Aviation Organization)

www.icao.int

Reference:

Title: Aviation Security Manual

Version: Tenth Edition, April 2017

Sector: Airborne System

Purpose: Definition of System Infrastructure and Supply Chain. It is also defined new threats and technological developments that have a bearing on the effectiveness of measures designed to prevent acts of unlawful interference.

Scope: Doc 8973 is a detailed document which provides guidance material to all the ICAO member states in achieving aviation security standards as described in Annex-17.

The guidance material covers on areas:

1. unpredictability,
2. behaviour detection techniques,
3. landside security, and
4. screening of persons other than passengers.
5. the evolving threat to civil aviation, and
6. inter alia, dangerous goods awareness training,
7. screening technology and equipment,
8. screening of vehicles and supplies, air cargo and mail secure supply chain measures, and
9. threat and risk assessment methodology.

Standard: ISO 27001

Organization: ISO: International Organization for Standardization
ISMS: Information Security Management Systems

www.iso.org

Reference:

Title: Information technology – Security techniques – Information security management systems – requirements

Version: ISO/IEC 27001:2013

Sector: no special sector

Purpose: Specification of a management system to bring information security under management control.

Scope: The standard deals with the following areas:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

Standard: ISO 27002

Title: Information technology – Security techniques – Code of practice for information security controls

Version: ISO/IEC 27002:2013

Sector: no special sector

Purpose: Provides best practice recommendations on information security controls.

Scope: The standard includes 5 introductory chapters and 14 main chapters. Each chapter describes information security controls and their objectives.

Standard: ISO 27035

Title: Information technology – Security techniques – Information security incident management

Version: ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016

Sector: no special sector

Purpose: The standard covers the processes for managing information security events, incidents and vulnerabilities.

Scope: This standard includes:

1. Plan and prepare
2. Detection and reporting
3. Assessment and decision
4. Responses
5. Lessons learned

The standard provides template reporting forms for information security events, incidents and vulnerabilities.

Standard: ISO 27036

Title: Information technology -- Security techniques -- Information security for supplier relationships

Version: ISO/IEC 27036:2013

Sector: no special sector

Purpose: It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships.
It provides additional guidance in the specific context of ICT supplies

Scope: This standard includes:

1. Information risks commonly arising from or relating to business relationships between acquirers and suppliers.
2. Governance and business management (e.g. operations, HR management, IT management, relationship management, metrics)
3. Information security management (e.g. information risk analysis and treatment, controls specification, architecture/design, strategy).
4. Information security controls (such as: chain of custody; compliance management; security training; procurement processes including anonymous and all-at-once acquisition; passing security requirements to upstream suppliers; quality management; supplier/relationship management; etc.)

Standard: EN ISO 16495

Organization: CEN: European Committee for Standardization

https://standards.cen.eu

Reference:

Title: Air Traffic Management - Information security for organisations supporting civil aviation operations

Version: 2019-07-03

Sector: Air Traffic Management

Purpose: Guidelines and general principles for the implementation of an information security management system in organisations supporting civil aviation operations

Scope: This document provides guidance based on EN ISO/IEC 27002:2017 applied to organisations supporting civil aviation, with a focus on air traffic management operations. This includes, but is not limited to, airspace users, airports and air navigation service providers. Not included are activities of the organisations that do not have any impact on the security of civil aviation operations like for example airport retail and service business and corporate real estate management. The basis of all guidance in this document is trust and cooperation between the parties involved in Air Traffic Management.

Standard: **ECAC Doc 30 – chapter 14**

Organization: ECAC / CEAC : European Civil Aviation Conference or Conférence Européenne de l'Aviation Civile

https://www.ecac-ceac.org

Reference:

Title: Chapter 14 – Cyber Security

Version:

Sector: Air Transport

Purpose: Compilation of best practice from aviation security, aviation safety and cyber security.

Scope: The document guidance based on procedural, physical, technical, logical and human elements needed the following:

1. Physical infrastructure - Layout, Definition of areas, Access procedures and Surveillance
2. IT system architecture – Network separation and Access rights
3. System and process design – No single points of failure, Redundancies and Human-machine interface

Standard: **Regulation (EC) 2320/2002 / Regulation (EC) No 300/2008**

Title: Common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

Sector: Aviation physical security

Purpose: Common basic standards for safeguarding civil aviation against acts of unlawful interference (article 4)

Scope: The regulation's provisions apply to all airports or parts of airports located in an EU country that are not used exclusively for military purposes. The provisions also apply to all operators, including air carriers, providing services at the aforementioned airports. It also applies to all entities located inside or outside airport premises providing services to airports. The regulation no 2320/2002 from 2002 introduced the requirement to have security checks for all passenger flights, also domestic.

Standard: **NIST SP800-30**

Organization: NIST

https://www.nist.gov/

Reference:

Title: Guide for Conducting Risk Assessment

Version: NIST SP 800-30 Revision 1, March 2012

Sector: Different sectors within US

Purpose: Purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.

Scope: Risk assessment is a key component of a holistic, organization-wide risk management process as defined in NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk.

This publication focuses on the risk assessment component of risk management—providing a step-by-step process for organizations on: (i) how to prepare for risk assessments; (ii) how to conduct risk assessments; (iii) how to communicate risk assessment results to key organizational personnel; and (iv) how to maintain the risk assessments over time.

Standard: **NIST SP800-53**

Title: Security and Privacy Controls for Information Systems and Organizations

Version: NIST SP 800-53 Revision 5 (Draft), August 2017

Sector: no special sector

Purpose: Is a set of standards and guidelines to help federal agencies and contractors meet the requirements set by the Federal Information

Security Management Act (FISMA).

Scope: The NIST SP 800-53 provides controls: the operational, technical, and management safeguards used by information systems to maintain the integrity, confidentiality, and security of federal information systems. SP 800-53 focuses on the controls which can be used along with the risk management framework outlined in 800-37. The controls are broken into 3 classes based on impact – low, moderate, and high.

NIST SP 800-53 also introduces the concept of security control baselines as a starting point for the security control selection process. NIST 800-53 compliance is a major component of FISMA compliance. It also helps to improve the security of our organization's information systems by providing a fundamental baseline for developing a secure organizational infrastructure.

Standard: NIST SP800-82

Title: Guide to Industrial Control Systems (ICS) Security

Version: Revision 2, March 2015

Sector: Different sectors within US

Purpose: Guide to Industrial Control Systems (ICS) Security, provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. SP 800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Scope: The scope of this document includes ICS that are typically used in the electric, water and wastewater, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries.

Performance Requirements - Real-time
Risk Management Requirements - Human safety is paramount, followed by protection of the process
Communications - Networks are complex and sometimes require the expertise of control engineers
Resource Constraints - industrial process may not have enough memory and computing resources
System Operation - proprietary operating systems, often without security capabilities built in
Change Management - Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained.

Standard: **ISA/IEC 62443**

Organization: ISA/IEC: International Standard Atmosphere/ International Electrotechnical Commission

https://www.isa.org https://www.iec.ch/

Reference:

Title: Industrial communication networks – Network and system security

Sector: Industrial

Purpose: The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to:

- hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Scope: ISA-62443 includes 14 standards in 4 groups related to information security.

1. General
- ISA-62443-1-1 Concepts and models
- ISA-TR62443-1-2 Master glossary of terms and abbreviations
- ISA-62443-1-3 System security conformance metrics
- ISA-TR62443-1-4 IACS security lifecycle and use-cases

2. Policies & Procedures
- ISA-62443-2-1 Security program requirements for IACS asset owners
- ISA-62443-2-2 IACS protection levels
- ISA-TR62443-2-3 Patch management in the IACS environment
- ISA-62443-2-4 Requirements for IACS service providers
- ISA-TR62443-2-5 Implementation guidance for IACS asset owners

3. System
- ISA-TR62443-3-1 Security technologies for IACS
- ISA-62443-3-2 Security risk assessment and system design
- ISA-62443-3-3 System security requirements and security levels

4. Component
- ISA-62443-4-1 Secure product development lifecycle requirements
- ISA-62443-4-2 Technical security requirements for IACS components

Standard: ED-201

Organization: EUROCAE/RTCA: European Organisation for Civil Aviation Equipment/Radio Technical Commission for Aeronautics

https://eurocae.net/

Title: Aeronautical Information System Security (AISS) Framework Guidance

Sector: Airborne System

Purpose: This document describes the overarching context of the shared responsibility for Aeronautical Information Systems Security (AISS) through the identification and description of topics, which have to be addressed. It also provides an introduction to all documents related to Aeronautical Information Systems Security (AISS) published by EUROCAE

Scope: Shared responsibility for Aeronautical Information Systems Security (AISS) for Civil Aviation by all relevant stakeholders. Safety of flight and maintaining the operation of the civil aviation infrastructure. Cyber security related to systems, processes, data and products. Concentrates on the shared cyber risk which is inherent in the situation where systems, processes, data or products are shared, or are passed from one organisation to another.

Standard: **ED-202A/DO-326A**

Organization: RTCA

https://www.rtca.org/

Reference:

Title: Airworthiness Security Process Specification

Version: ED-202A/DO-326A, August 2014

Sector: Airborne System

Purpose: This document is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of intentional unauthorized electronic interaction can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of intentional unauthorized electronic interaction (the “What”).

Scope: Guidance to handle the information security threat to aircraft safety. Compliance objectives to handle the cyber security threat to aircraft safety and is intended to be used in conjunction with other applicable guidance material, including SAE ARP4754A/ED-79, DO-178C/ED-12C, and DO-254/ED-80 and with the advisory material associated with AMC 25.1309 but may be applicable to CS-23, CS-27, CS29, CS-E

Standard: **ED-203A/ DO-356A**

Title: Airworthiness Security Methods and Considerations

Version: ED-203A/DO-356A, June 2018

Sector: Airborne System

Purpose: This document provides a set of methods and guidelines that may be used within the airworthiness security process defined in ED-202A/ DO-326A.

Scope: Guidelines, methods and tools used in performing an airworthiness security process. Acceptability of the airworthiness security risk and the design and verification of the airworthiness security attributes as related to system safety and airworthiness. Other aspects of information security that do not affect the airworthiness security of the type design are excluded.

Standard: ED-204/ DO-355

Title: Information Security Guidance for Continuing Airworthiness

Version: ED-204/ DO-355, June 2014

Sector: Airborne System

Purpose: ED-204 provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration and deconstruction.

Scope: Activities that need to be performed in operation and maintenance of the aircraft when it comes to cyber security. Guidance for the operation and maintenance of aircraft by organizations and personnel involved in these tasks.

Standard: ED-205

Title: Process Standard for Security Certification and Declaration of ATM ANS Ground Systems

Version: ED-205, March 2019

Sector: Airborne System

Purpose: Secure the ATM / ANS ground system

Scope: ED-205 provides a process to assess the extent to which the Air traffic management (ATM)/ air navigation service (ANS) ground systems are appropriately secured for use. The process is be used to identify, evaluate and manage impacts on safety, operational delivery and other commercial concerns. This document is a resource for certification or declaration of conformity with applicable security requirements.

Standard: ARINC 664 (Part 5)

Organization: ARINC: Aeronautical Radio Incorporated

https://www.arinc.com

Title: Aircraft Data Network: Mobility and Network Security (Part 5)

Sector: Airborne System

Purpose: Defines the use of a deterministic Ethernet network as an avionic databus in modern aircraft like the Airbus A380, Sukhoi Superjet 100, the Bombardier CSeries, and the Boeing 787 Dreamliner.

Scope: Specification for a deterministic aircraft data network bus for aeronautical, railway and military systems. Based on standard IEEE 802.3 extended by adding Quality of Service (QoS) and deterministic behaviour with a guaranteed dedicated bandwidth. Avionics Full-Duplex Switched Ethernet (AFDX) network.

Standard: ARINC 811

Title: Commercial Aircraft Information Security Concepts of Operation and Process Framework

Sector: Airborne System

Purpose: Provides a common understanding of information security concepts as they relate to airborne networks and provides a framework for evaluating the security of airborne networked systems.

Scope: Understanding of aircraft cyber security. Help to develop aircraft cyber security operational concepts. Aircraft information security process framework relating to airline operational needs. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.

Standard: ARINC 823 part 1

Title: Datalink Security/ ACARS Message Security (AMS)

Sector: Airborne System

Purpose: AMS security framework, services, algorithms, Message protocol Security protocol, and protocol message format

Scope: The ARINC 823 Part 1 permits ACARS datalink messages to be exchanged between aircraft and ground systems in a secure, authenticated manner using a uniform security framework. The security framework described herein is based on open international standards that are adapted to the ACARS datalink communications environment.

ARINC 823 Part 1, ACARS Message Security, sets forth the provisions available to airlines and Datalink Service Providers (DSPs) to protect ACARS messages that are exchanged over traditional ACARS air-ground datalinks (VHF, HF, and SATCOM) and ground-ground communication networks.

Standard: **ARINC 823 part 2**

Title: Datalink Security/ AMS Key Management

Sector: Airborne System

Purpose: Life cycle key/ certificate management guidance for implementers and operators

Scope: The ARINC 823 Part 2 is to provide recommended guidance and provisions for ACARS Message Security (AMS) key management. The key management framework described herein is based on open international standards that are adapted to the ACARS datalink communications environment.

ARINC 823 Part 2 sets forth the guidance and provisions available to airlines and datalink service providers for the life-cycle management of the cryptographic keys that are necessary for proper and secure operation of ACARS Message Security. The security provisions contained in Part 1 of this specification supports the use of either public/private (i.e., asymmetric) keys or a shared secret (i.e., symmetric) key for secure session initiation and key establishment between communicating peer aircraft and ground entities. This document provides guidance and provisions appropriate for the life-cycle key management of each approach.

Standard: **ATA Spec 42**

Organization: A4A (Airline for America, former ATA)

https://www.airlines.org

Reference:

Title: Aviation Industry Standards for Digital Information Security

Version: Revision 2018.1

Sector: Airborne System

Purpose: To satisfy the identity assurance and data integrity requirements of the civil aviation industry, identity management solutions, based on Public Key Infrastructure (PKI) technology must be deployed.

Scope: Digital aircraft, connected aircraft with extensive requirements for external interaction. Aircraft avionics communicating with a ground station, or a passenger in the aircraft accessing a service using the Internet, great care must be taken to ensure that only legitimate communication or 'information transfer' is occurring. Requires the deployment of identity management solutions, based on Public Key Infrastructure (PKI) technology. PKI is a set of policies, practices, and technologies used to create a trust framework for securing digital data and authenticating digital identities. ATA Specification 42 describes the PKI requirements and specifications for the civil aviation industry.

BDLI FACHAUSSCHUSS CYBERSICHERHEIT

aes AEROSPACE EMBEDDED SOLUTIONS

AIRBUS

AKKA PASSION FOR TECHNOLOGIES

BDI

BDSV

CIMPA PLM Services a Sopra Steria company

DLR

ESG

HENSOLDT Detect and Protect.

IABG

ILFA

OHB

philotech We love engineering.

ROHDE&SCHWARZ Make ideas real

SCISYS

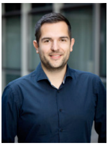
sogeti Part of Capgemini

THALES

TÜV NORD

umlaut

POINT OF CONTACT



Robert Friebe
Manager digitization, cyber security and UAS

German Aerospace Industries
Association (BDLI)
+49 (0)30 206140-0
contact@bdli.de
www.bdli.de
January 2020