भारतीय मानक **IS 19031 : 2023**

Indian Standard

मानव रहित विमान प्रणाली — साइबर सुरक्षा

Unmanned Aircraft Systems — Cybersecurity

ICS 49.020, 35.030

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुर शाह ज़फर मार्ग, नई दिल्ली - 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110002
www.bis.gov.in www.standardsbis.in

November 2023 **Price Group 7**

Unmanned Aerial Vehicles Sectional Committee, TED 32

FOREWORD

This Indian Standard was adopted by the Bureau of Indian Standards, after the draft finalized by the Unmanned Aerial Vehicles Sectional Committee had been approved by the Transport Engineering Division Council.

Since unmanned aircraft system is prone to cyber-attacks and can be used for unethical purposes, cyber security plays a significant role for safety and security of all the involved stakeholders. As per the guidelines laid down in this standard, the user should identify the risk involved in the operation of the UAS as per the mission profile and need to identify preventive actions as per the identified risk.

Other international cyber security standards/guidelines for UAS such as joint authorities for rulemaking of unmanned systems (JARUS) guidelines on specific operations risk assessment (SORA), MIL 882 E, ARP 4761 are also available and may be referred by the operator/manufacturer.

The composition of the Committee responsible for the formulation of this standard is given in Annex A.

For the purpose of deciding whether a particular requirement of this standard is complied with the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 2022 ‘Rules for rounding off numerical values (*second revision*)’. The number of significant places retained in the rounded-off value should be the same as that of the specified value in this standard.

Indian Standard

UNMANNED AIRCRAFT SYSTEMS — CYBERSECURITY

1 SCOPE

This Indian Standard specifies cyber security requirements with respect to Unmanned Aircraft Systems (UAS) for cyber security features during design and development, manufacturing, operations and cyber security artefacts at the end-of-life cycle.

2 REFERENCES

The standards given below contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of these standards:

IS No.	*Title*
IS/ISO 9001 : 2015	Quality management systems — Requirements (*fourth revision*)
IS/ISO 27001 : 2022	Information security cyber security and privacy protection information security management systems requirements — Requirements
IS/ISO 27002 : 2022	Information security cyber security and privacy protection information security controls
IS/ISO 31000 : 2018	Risk management — Guidelines

3 GENERAL CONSIDERATIONS

This document applies to all elements that help in achieving the required level of assurance for unmanned aircraft systems. Unmanned aircraft systems (UAS) include unmanned aircraft, controllers, UAS traffic management systems (UTM), UAS service suppliers (USS) and ground control systems of the UAVs. This document will also apply to UAS manufacturers and suppliers of parts or UAS as whole, service providers and any such entity or organization that is a part of UAS ecosystem. Defense-in-depth using a layered approach in choosing the requirements may be used to mitigate the identified risks or to achieve an acceptable level of risk.

4 OVERALL CYBER SECURITY MANAGEMENT

4.1 To enable cyber security management in projects related to unmanned aircraft systems, an associated organization requires instituting and maintaining a cyber security culture through governance and awareness. The organization shall endeavor to maintain cyber security at the organizational level thereby ensuring cyber security of its products and services. A typical diagram showing various aspects of cyber security is shown in Fig. 1.

NOTE — An organization refers to an entity, which claims to be a manufacturer, OEM, distributor, supplier, provider of maintenance services, traffic management services including but not limited to parts, peripherals and allied services for unmanned aircraft services (UAS).

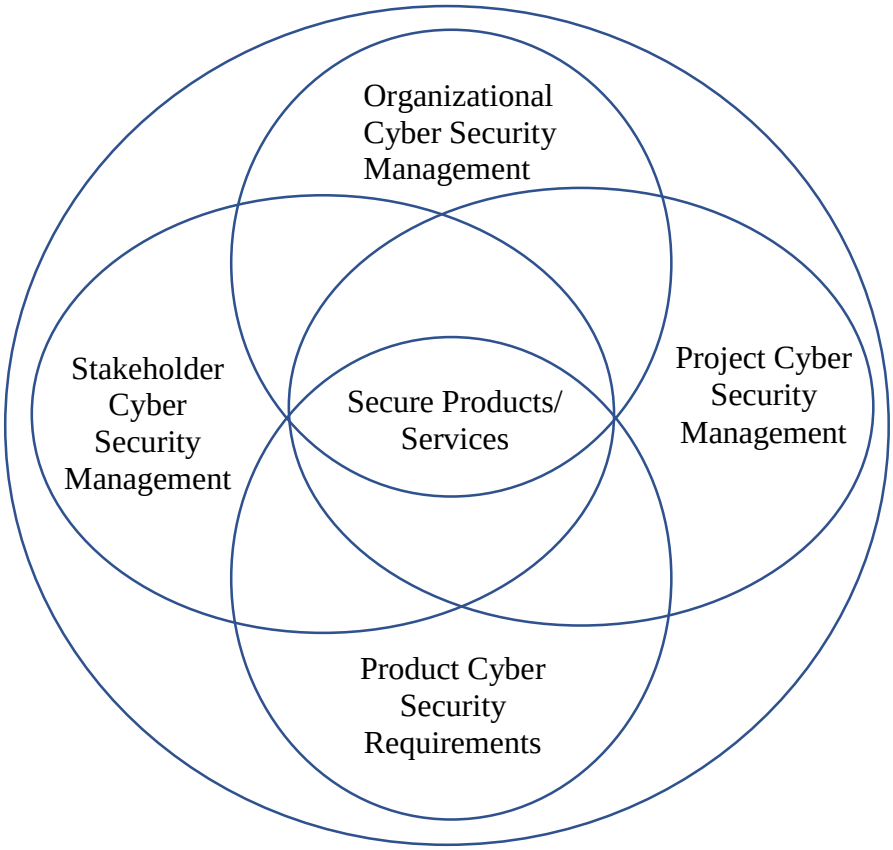

FIG 1. OVERALL CYBER SECURITY MANAGEMENT

4.2 The information security management of the organization shall be in compliance with IS/ISO 27001 : 2022 and IS/ISO 27002 : 2022

4.3 The organization shall have project level cyber security management practices in place as described in subsequent clauses for each project.

4.4 The organization shall have product/service level cyber security management practices and features in place as described in subsequent clauses for each product/service.

4.5 The organization shall maintain separate cyber security programs for the organization, projects and its products/services.

4.6 The organization shall have a documented public policy defining the maintenance of privacy of data collected and handled by the organization while providing UAS products and services.

4.7 The organization shall have a documented public policy defining the data retention, storage and geographical location of storage of data collected and handled by the organization while providing UAS products and services.

4.8 The organization shall have a documented public policy on disclosure of information related to cyber security incidents, vulnerabilities reported, and fixes issued.

4.9 The organization shall follow IS/ISO 9001 : 2015 with respect to its quality management system of cyber security components of UAS products and service.

4.10 The cyber security risk management system shall be in accordance with IS/ISO 31000 : 2018.

4.11 The organization shall define a risk assessment methodology for its UAS products and services to ensure that overall risk is at an acceptable level while considering the following in the least along with operational parameters:

a) Kinetic energy achievable by the UAV;
b) Probability of injury to people/livestock on ground;
c) Probability of crashing into another aircraft;
d) Potential violation of privacy;
e) Damage to critical infrastructure;

f) Loss of control over the UAV;

g) Damage to the environment; and

h) Functional safety.

4.12 The organization shall establish organization specific rules and policies which shall enable implementation and execution of the requirements of this document and allied activities which can enable such execution.

5 PROJECT LEVEL CYBER SECURITY MANAGEMENT

5.1 Overview

This clause describes the cyber security requirements of the development process.

5.1.1 The organization shall define rules and processes for project level cyber security management.

5.1.2 The organization shall document the following with respect to every project:

a) Cyber security plan; and

b) Identification and assignment of cyber security roles and responsibilities.

5.1.3 The project cyber security planning shall consist of following stages whose result should be documented and used as an input to the subsequent stage:

a) Threat and risk assessment. this stage shall use product/service requirements as an input;

b) Development of security concept;

c) Composition of security requirements;

d) Implementation of security requirements;

e) Functional testing of security requirements; and

f) Verification and validation of security requirements.

5.2 Threat and Risk Assessment

Risk assessment shall be carried out and documented. The document shall consist of, but not limited to, the following sections.

5.2.1 Security goals shall be identified and defined.

5.2.2 All threats scenarios, according to the operational and safety requirements based on the risk assessment methodology shall be identified and documented.

5.2.3 A risk evaluation matrix based on consequences and likelihood of occurrence shall be documented.

5.2.4 Risk acceptance criteria shall be defined with justification.

5.2.5 The risk assessment process shall bring out a list of risks, ordered in descending order of risks, which need to be addressed during development of security concept.

5.3 Security Concept

Security concept makes a case for inclusion of cyber security requirements based on the threat and risk assessment. It should define the security architecture, design, and implementation.

5.3.1 The security concept shall define system level requirements for ensuring security of information and information technology in the product and the environment.

5.3.2 The security concept shall define both technical and organizational measures to ensure security of information and information technology.

5.3.3 The security concept shall explain the inclusion of requirements vis-à-vis the assessed risk.

5.3.4 The security concept shall list and explain the residual risks.

5.3.5 The security concept shall define the cyber security lifecycle management of product. It shall include, but not limited to, the following details:

a) Secure provisioning of immutable artefacts;

b) Secure update process;

c) Secure field return analysis procedures; and

d) Secure decommissioning of cyber security artefacts.

5.3.6 The security concept shall map regulatory and legal requirements to the system level cyber security requirements.

5.4 Functional Testing

The functionality of cyber security requirements has to be tested to confirm that the desired functionality has been achieved.

5.4.1 Functional testing of cyber security requirements shall be carried out and documented.

5.4.2 The functional testing methods, tools and setup shall be maintained over the lifecycle of the product.

5.4.3 The functional tests may be carried out by the development teams.

5.5 Verification and Validation of Security Requirements

The verification and validation of security requirements is to be carried out on completion of functional tests by an independent verification team.

5.5.1 Verification and validation of the product/services should be carried out by an independent team which is different from the development team whose result should be a list of vulnerabilities and security issues found during the verification and validation tests. In case the verification and validation is carried out by an internal team, a declaration to that effect shall be added at the beginning of the report.

5.5.2 The verification and validation report shall consist of, but not limited to, following sections:

a) Scope of test;
b) Test methodology;
c) Method used for severity scoring of vulner-abilities and security issues;
d) Hardware and software versions (along with a digital digest, where possible) of component under test; and
e) A summary of vulnerabilities found along with their severity and recommendations.

5.5.3 The verification and validation test shall consist of at least one of the following methods depending on the use case mentioned against each:

a) Penetration tests (white box/grey box/black box) for hardware and software components;
b) Fuzz tests (white box/grey box/black box) for protocols and software components; and
c) Code walk through for software components.

5.6 Cyber Security Roles and Responsibilities

The Roles and responsibilities for carrying out cyber security management of the projects needs to be defined.

5.6.1 The organization shall define rules and processes for assigning roles and responsibilities for carrying out cyber security activities in UAS engineering projects.

5.6.2 The organization shall ensure that competent personnel are assigned the roles and responsibilities for carrying out cyber security activities in UAS engineering projects.

5.6.3 The organization shall ensure that adequate resources are allocated in the project plan for carrying out activities related to cyber security management.

5.6.4 A project shall have identified and competent personnel who are responsible for:

a) Carrying out threat and risk assessment;
b) Defining acceptable risk;
c) Authorizing signing off residual risk; and
d) Coordinating security-related aspects of a project.

6 PRODUCT/SERVICES CYBER SECURITY REQUIREMENTS

This clause brings out the baseline cyber security requirements for the UAS products and services.

6.1 Access Controls

Based on the outcome of risk assessment, the product and services shall have necessary access controls for enforcing organization policies/directives and to prevent unauthorized access.

6.1.1 The product/services should have role-based access controls.

6.1.2 Least privileged permissions for all users/roles shall be implemented.

6.1.3 Access to privileged operations and information should be restricted.

6.1.4 The product/services may have mandatory access controls.

6.1.5 The product/services may have discretionary access controls.

6.1.6 A list of procedures and methods for access to the product/services including disabled access methods should be documented and provided as a part of the overall documentation.

6.1.7 Privileged access to the device, if any, should be documented and restricted to a controlled group of users, whose records should be maintained over the lifecycle of the product.

6.2 Authentication and Identification Controls

Controls under this clause are used to uniquely identify the users. These controls are closely tied to access controls and hence have to be commensurate with the risk assessed due to such controls and shall be chosen accordingly.

6.2.1 A list of supported Authentication and Identification schemes shall be provided.

6.2.2 The information used to authenticate a user/ service shall always be stored in an encrypted form.

6.2.3 For critical functions, two factor authentication may be utilized.

For that is Pilot may plug in his digitally signed license along with existing authentication controls to enable propulsion mechanism of the UAV.

6.2.4 Identifiers, which uniquely identify a device, a product, manufacturer, supplier or a service, should be stored in an immutable (unchangeable) way.

6.2.5 For all authentication sessions, idle timeout shall be enforced.

6.2.6 Maximum time for all authenticated sessions should be defined and force re-authentication should be enforced.

6.2.7 Maximum number of authentication attempts should be kept to minimum and a lock out shall be enforced on exceeding maximum number of unsuccessful attempts.

6.2.8 Mutual authentication may be used.

6.2.9 A list of default accounts along with passwords or lack of thereof shall be provided.

6.3 Audit and Accountability

Based on risk assessment, data to be logged and granularity of logging shall be determined.

6.3.1 Log shall be maintained by all the UAS products and services.

6.3.2 The data logging capacity shall be at least twice the endurance of the UAV.

6.3.3 A protected time source for time stamping logs referenced to co-ordinated universal time (UTC) shall be maintained.

6.3.4 All devices of a system shall be in sync with respect to time.

6.3.5 A redundant time source may be employed.

6.3.6 All critical logs shall be simultaneously stored on the UAS and a location external to the UAS.

6.3.7 The log shall consist of:

a) Unique ID of the log;

b) Timestamp;

c) Unique identifiers with respect to communication (origin, destination, port etc.) [network logs];

d) Unique identifiers with respect to process [process identifier (PID)], parent process identifier (PPID), name of the process, etc.) [system logs]; and

e) Unique identifiers with respect to the user and privileges (username, root, administrator etc.) [system logs]

6.3.8 Detailed documentation shall be provided with respect to logs designed into the systems/products as a part of the end user documentation which shall include:

a) Method/process for accessing/extracting logs;

b) Location and names of log files;

c) Tools/software required to understand the logs; and

e) Mapping of logs to security critical processes of services/products.

6.3.9 Redundancy in logging shall be ensured.

6.4 Awareness and Training

6.4.1 A cyber security manual shall be provided for the purpose of providing awareness and training about cyber security features of the products/services.

6.4.2 The cyber security manual shall also include potential risks taken into consideration during risk assessment and corresponding cyber security measures included in the product/services.

6.4.3 The cyber security manual shall include information about the concurrent Information Technology and Privacy laws of the land.

6.4.4 The cyber security manual may provide information for users to detect potential signs of information security incidents.

6.5 Configuration Management

Configuration management is used to ensure that a baseline configuration is created, and version control is maintained for the configuration used in products/service.

6.5.1 A cyber security bill of material comprising of a list of all the programming elements in the product, software used and their dependencies along with version numbers shall be provided along with the products.

6.5.2 All unnecessary ports and interfaces shall be disabled and a list of all such disabled ports and interfaces shall be provided.

6.5.3 All unused and unnecessary software shall be removed.

6.5.4 A list of services/daemons running on the system shall be provided along with their use cases.

6.5.5 All the software used shall be patched for known vulnerabilities.

6.5.6 Any upgrades and updates resulting in a change of configuration of the device shall be intimated with an indication of requirement of security impact analysis.

6.5.7 Access controls with restrictions shall be in place for carrying out any changes to hardware, software, and firmware.

6.5.8 A list of configuration settings should be provided which shall have an impact on security according to the risk assessment.

6.5.9 Wherever feasible, the least functionality principle may be utilized in determining functionalities of multifunctional components.

6.5.10 A baseline security document should be provided along with the product documentation.

6.5.11 Regulatory requirements shall be identified and implemented in a secure way such that they can neither be altered nor tampered with.

6.5.12 Only legitimate software/firmware whose integrity and authenticity has been verified shall be allowed to be executed.

6.5.13 Electronic control through software over strobe lights shall not be possible.

6.6 Contingency Planning

Depending upon the risk assessment contingency controls shall be in place.

6.6.1 A list of critical functions shall be listed for which redundancy has been provided according to the risk assessment, that is communication channels, global navigation satellite system (GNSS) etc.

6.6.2 Copies of firmware and a provision to securely reinstall the baseline software as permitted by regulatory agencies may be provided.

6.6.3 A contingency plan document indicating the measures in place in hardware and software for the following contingencies shall be provided along with the product/service documentation:

a) Residual power approaches minimum permissible limit before it cannot return back home;
b) Loss of GNSS;
c) Loss of communication link; and
d) Loss of functionality of critical navigation equipment such as gyroscope, altimeter

6.7 Cyber Security Incident Response

Based on the risk assessment incident response controls shall be provided to enable incident response and investigation thereon.

6.7.1 A manual comprising of information for incident response shall be provided as of system documentation. The document shall consist of a minimum requirement of:

a) Definition of cyber security incident;
b) Features included in the product facilitating incident response;
c) Storage location of cyber security incident logs and various methods/procedures to access them; and

6.7.2 The features included for incident response shall be tamper proof.

6.7.3 Based on the threat and risk analysis the frequency of export of all the security related logs to ground station/alternate location such as cloud shall be determined.

6.8 Maintenance

6.8.1 A schedule of maintenance for information security components shall be provided, that is backup of logs, update and upgrade of firmware etc.

6.8.2 A record of all maintenance activities carried out on information technology components shall be logged.

6.8.3 An intended period of support for patches and updates shall be declared for all the software and hardware products.

6.8.4 A secure update process shall be implemented for patching and upgradation of firmware.

6.8.5 Downgrade of firmware shall not be possible.

6.8.6 Firmware shall remain tamper proof and any changes to firmware through secure upgrade process shall be logged and communicated to users through alternate means of communication.

6.8.7 A clause shall be included in the service level agreement/sale agreement/purchase offer for communicating information regarding reported/ discovered vulnerabilities with critical and high severity rating including means of communication and time limit for such intimation.

6.9 Physical and Environmental Protection

Based on risk assessment, physical and environmental controls shall be included to achieve the required assurance levels.

6.9.1 Physical barriers to security related components should be provided.

6.9.2 A list of physically disabled/protected ports/interfaces shall be provided, that is joint test action group (JTAG) ports, epoxy coated via points etc.

6.9.3 All the information technology components should be tested for environmental resilience.

6.9.4 All the information technology components shall be suitably housed to protect them from environmental and accidental damage.

6.9.5 Physical tamper protection features may be employed.

6.9.6 The surface package mount for integrate chips especially the baseband processors and microprocessors/microcontrollers, peripheral modules (wifi, GNSS etc) utilized may be chosen in such a way to deter physical access to the leads of integrated chips that is ball grid array (BGA), plastic ball grid array (PBGA), land grid array (LGA) etc.

6.9.7 The traces carrying onboard communication on controller boards may route through inner layers to deter tapping of onboard communication.

6.10 System and Services Acquisition

Based on the outcome risk assessment system, service acquisition controls shall be chosen to address the risk appropriately.

6.10.1 All discrete information technology components used as building blocks for the products/service shall be individually assessed for their security features.

6.10.2 Secure configurations for discrete information technology components shall be provided for the purpose of reconfiguration on replacement/post maintenance.

6.10.3 Functional properties of security controls included in the product/services should be provided to the end users.

6.10.4 A list of functions, open ports and protocols used and supported by the product/service for external interfaces should be provided as a part of the system documentation.

6.11 Communication Protection

6.11.1 Communication with external entities such as servers/service providers etc. shall happen post mutual authentication. Communication between internal and external components shall always be encrypted.

6.11.2 The communication channels shall be resistant to record and replay attacks.

6.11.3 All remote commands to the drone shall always be encrypted.

6.12 Integrity Protection

6.12.1 The systems shall implement an immutable root of trust.

6.12.2 The systems shall not operate prior to verification of integrity of firmware.

6.12.3 The verification of integrity of all components shall be anchored to root of trust.

6.13 Privacy Protection

6.13.1 The privacy controls provided in the system shall be documented separately as a part of system documentation. Consent of the user shall be sought prior to seeking the private data for storage.

6.13.2 Policy for utility, storage and sharing of private data shall be documented and provided as a part of system documentation.

6.13.3 Private data shall be pseudonymised.

6.13.4 A flashing strobe light of blue colour shall be implemented when the UAV is recording visual data.

7 STAKEHOLDER CYBER SECURITY MANAGEMENT

7.1 An organization shall have documented process to identify all stakeholders who can influence cyber security.

7.2 All stakeholder organizations shall be required to be compliant to IS/ISO 27001 as determined by the assessment process.

7.3 All components supplied by the stakeholders shall be assessed for security assurance.

ANNEX A

(*Foreword*)

COMMITTEE COMPOSITION

Unmanned Aerial Vehicles Sectional Committee, TED 32

Organization	*Representative(s)*
Indian Institute of Science, Bengaluru	DR S. N. OMKAR **(*Chairperson*)**
Adani Aerospace and Defence Limited, Bengaluru	SHRI SAMPATHKUMARAN S. T. SHRI SWAPNIL JALUNDHWALA (*Alternate*)
Aerospace and Aviation Sector Skill Council, Bengaluru	CDR A. K. N. BALAJI
Airdonex Technologies Private Limited, Chennai	SHRI CHANDRU RAJENDRAN
Airports Authority of India, New Delhi	SHRI HARSHAD VIJAY KHATAVKAR
Anna University, Chennai	DR K. SENTHIL VADIVU
Centre for Military Air worthiness and Certification, Bengaluru	LN RAGHAVENDRA SHRI ADITYA KUMAR MISHRA (*Alternate*)
Collins Aerospace, Bengaluru	SHRI PRASANNA RAMAMURTHY
CyPhySignals India Private Limited, Bengaluru	SHRI D. SRINIVASAN
DeTect Technologies, Chennai	SHRI KARTHIK RAJASEKARAN SHRI G. D. SUNIL (*Alternate*)
Directorate General of Aeronautical Quality Assurance, Ministry of Defence, New Delhi	SHRI RAHUL GUPTA SHRI MUKESH CHAND MEENA (*Alternate*)
Directorate General of Civil Aviation, New Delhi	SHRI MANISH GUPTA SHRI PRAVEEN KUMAR SINGH (*Alternate*)
Drone Federation of India, New Delhi	SHRI SMIT SHAH SHRI VIPUL SINGH (*Alternate)*
Hindustan Aeronautics Limited, Bengaluru	SHRIMATI NISHA GANESH SHRI PRATAP PANDA (*Alternate*)
Honeywell Technology Solutions, Bengaluru	DR JEPPU YOGANANDA
Idea Forge Technology Private Limited, Mumbai	SHRI RAGHAV MALLICK
Indhra Dhanush Autonomous Platforms, Mangaluru	SHRI NEVILLE RODRIGUES
Indian Institute of Technology Bombay, Mumbai	DR HEMENDRA ARYA
Indian Institute of Technology Kanpur, Kanpur	DR ABHISHEK
Indian Space Research Organization, Bengaluru	SHRI MANISH SAXENA
Institute of Electrical and Electronics Engineers Standards Association	SHRI SRIKANTH CHANDRASEKARAN
International Air Transport Association	SHRI PRASHANT SANGLIKAR
International Centre for Automotive Technology, Manesar	SHRI DEVESH PAREEK
International Institute of Aviation, Bengaluru	SHRIMATI SMILEY SOOD SHRI SUMEET SUSEELAN (*Alternate*)

Organization	*Representative(s)*
LDRA Technology Private Limited, Bengaluru	SHRI SHINTO JOSEPH
Next Leap Aeronautics, Bengaluru	SHRI GAJENDRA KASHYAP
Nokia India, Gurugram	SHRI SATISH KANUGOVI SHRI SAURABH SINGH (*Alternate*)
North-Eastern Space Applications Centre, Umiam	SHRI CHIRAG GUPTA
Quality Council of India, New Delhi	DR MANISH PANDE SHRI C. S. SHARMA (*Alternate*)
Reverence Tech, Mumbai	SHRI NITISH SAWANT
Robert Bosch Engineering and Business Solutions, Bengaluru	SHRIMATI PRIYAMVADHA VEMBAR LT CDR P. V. J. HARSHA (*Alternate*)
Sanganak Labs, Bengaluru	SHRI RAJ ASHISH
System Level Solutions (India) Private Limited, Anand	SHRI ANAND PUROHIT
Vidhya Sangha Technology, Bengaluru	SHRI A. T. KISHORE
Wavekids India, Bengaluru	SHRIMATI ANIMA AGARWAL
In Personal Capacity (*21/2 MG Road,Craig Park Layout, Bangalore - 560001*)	SHRI RAEJUS JOB
BIS Directorate General	SHRI P. V. SRIKANTH, SCIENTIST 'D'/JOINT DIRECTOR AND HEAD (TRANSPORT ENGINEERING) [REPRESENTING DIRECTOR GENERAL (*Ex-officio*)]

Member Secretary
SHRI SHIVAM AGGARWAL
SCIENTIST 'C'/DEPUTY DIRECTOR
(TRANSPORT ENGINEERING), BIS

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the website-www.bis.gov.in or www.standardsbis.in.

This Indian Standard has been developed from Doc No.: TED 14 (16194).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: 601/A, Konnectus Tower -1, 6th Floor, DMRC Building, Bhavbhuti Marg, New Delhi 110002	2323 7617
Eastern	: 8th Floor, Plot No 7/7 & 7/8, CP Block, Sector V, Salt Lake, Kolkata, West Bengal 700091	2367 0012 2320 9474
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg, Chandigarh 160019	265 9930
Southern	: C.I.T. Campus, IV Cross Road, Taramani, Chennai 600113	2254 1442 2254 1216
Western	: Plot No. E-9, Road No.-8, MIDC, Andheri (East), Mumbai 400093	2821 8093

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. CHANDIGARH. CHENNAI. COIMBATORE. DEHRADUN. DELHI. FARIDABAD. GHAZIABAD. GUWAHATI. HIMACHAL PRADESH. HUBLI. HYDERABAD. JAIPUR. JAMMU & KASHMIR. JAMSHEDPUR. KOCHI. KOLKATA. LUCKNOW. MADURAI. MUMBAI. NAGPUR. NOIDA. PANIPAT. PATNA. PUNE. RAIPUR. RAJKOT. SURAT. VISAKHAPATNAM.

Published by BIS, New Delhi