



# FINAL DRAFT International Standard

## ISO/IEC FDIS 19790

### Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:  
**2024-11-26**

Voting terminates on:  
**2025-01-21**

iTeh Standards  
(<https://standards.itih.ai>)  
Document Preview

[ISO/IEC FDIS 19790](https://standards.itih.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790)

<https://standards.itih.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/IEC FDIS 19790](https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790)

<https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>17</b>
<b>5 Cryptographic module security levels</b> .....	<b>18</b>
5.1 General.....	18
5.2 Security level 1.....	18
5.3 Security level 2.....	19
5.4 Security level 3.....	19
5.5 Security level 4.....	20
<b>6 Functional security objectives</b> .....	<b>21</b>
<b>7 Security requirements</b> .....	<b>21</b>
7.1 General.....	21
7.2 Cryptographic module specification.....	24
7.2.1 Cryptographic module specification general requirements.....	24
7.2.2 Types of cryptographic modules.....	24
7.2.3 Cryptographic boundary.....	24
7.2.4 Module operations.....	25
7.3 Cryptographic module interfaces.....	27
7.3.1 Cryptographic module interfaces general requirements.....	27
7.3.2 Types of interfaces.....	27
7.3.3 Categories of interfaces.....	27
7.3.4 Plaintext trusted path.....	28
7.3.5 Protected internal paths.....	29
7.4 Roles, services, and authentication.....	29
7.4.1 Roles, services, and authentication general requirements.....	29
7.4.2 Roles.....	29
7.4.3 Services.....	30
7.4.4 Authentication.....	31
7.5 Software/firmware security.....	33
7.5.1 Software/firmware security general requirements.....	33
7.5.2 Security level 1.....	34
7.5.3 Security level 2.....	34
7.5.4 Security levels 3 and 4.....	35
7.6 Operational environment.....	35
7.6.1 Operational environment general requirements.....	35
7.6.2 Clause applicability.....	36
7.6.3 Operating system requirements for modifiable operational environments.....	37
7.7 Physical security.....	39
7.7.1 Physical security embodiments.....	39
7.7.2 Physical security general requirements.....	40
7.7.3 Physical security requirements for each physical security embodiment.....	42
7.7.4 Environmental failure protection/testing.....	43
7.7.5 Environmental failure protection features.....	43
7.7.6 Environmental failure testing procedures.....	44
7.8 Non-invasive security.....	44
7.8.1 Non-invasive security general requirements.....	44
7.8.2 Security levels 1 and 2.....	45
7.8.3 Security level 3.....	45
7.8.4 Security level 4.....	45

# ISO/IEC FDIS 19790:2024(en)

7.9	Sensitive security parameter management.....	45
7.9.1	Sensitive security parameter management general requirements.....	45
7.9.2	Random bit generators.....	45
7.9.3	Sensitive security parameter generation.....	46
7.9.4	Automated sensitive security parameter establishment.....	46
7.9.5	Sensitive security parameter entry and output.....	46
7.9.6	Sensitive security parameter storage.....	47
7.9.7	Sensitive security parameter zeroization.....	47
7.10	Self-tests.....	48
7.10.1	Self-test general requirements.....	48
7.10.2	Security levels 3 and 4.....	49
7.10.3	Pre-operational self-tests.....	49
7.10.4	Conditional self-tests.....	50
7.11	Life-cycle assurance.....	53
7.11.1	Life-cycle assurance general requirements.....	53
7.11.2	Configuration management.....	53
7.11.3	Design.....	54
7.11.4	Finite state model.....	54
7.11.5	Development.....	55
7.11.6	Vendor testing.....	56
7.11.7	Delivery and operation.....	56
7.11.8	Guidance documents.....	58
7.12	Mitigation of other attacks.....	58
7.12.1	Mitigation of other attacks general requirements.....	58
7.12.2	Security levels 1, 2 and 3.....	58
7.12.3	Security level 4.....	59
<b>Annex A (normative)</b>	<b>Documentation requirements.....</b>	<b>60</b>
<b>Annex B (normative)</b>	<b>Cryptographic module security policy.....</b>	<b>66</b>
<b>Annex C (normative)</b>	<b>Approved security functions.....</b>	<b>72</b>
<b>Annex D (normative)</b>	<b>Approved sensitive security parameter generation and establishment methods.....</b>	<b>74</b>
<b>Annex E (normative)</b>	<b>Approved authentication mechanisms.....</b>	<b>75</b>
<b>Annex F (normative)</b>	<b>Approved non-invasive attack mitigation test metrics.....</b>	<b>76</b>
<b>Annex G (normative)</b>	<b>Module secure development, manufacturing and operation.....</b>	<b>77</b>
	<b>Bibliography.....</b>	<b>78</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 19790:2012), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19790:2012/Cor 1:2015.

The main changes are as follows:

- [Clauses 3, 4](#) and [5](#) have been refined and updated to reflect changes in requirements in [Clause 7](#);
- the language in [Clause 6](#) has been refined and modernized;
- in [Clause 7](#), the requirements have been reworded and rearranged for clarity. New requirements have been added, and redundant or unnecessary requirements removed;
- [Annexes A](#) and [B](#) have been updated to reflect changes in requirements in [Clause 7](#);
- [Annexes C, D](#) and [E](#) have been restructured and updated in line with standards published since the previous edition, as well as with examples of rate limiting methods;
- [Annex F](#) has been updated with the inclusion of ISO/IEC 17825; and
- new [Annex G](#) on module secure development, manufacturing and operation has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction

In information technology there is an ever-increasing need to use cryptographic mechanisms, such as for the protection of data against unauthorized disclosure or manipulation, for entity authentication and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

This document provides four increasing qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels defined in this document. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include:

- cryptographic module specification;
- cryptographic module interfaces;
- roles, services, and authentication;
- software/firmware security;
- operational environment;
- physical security;
- non-invasive security;
- sensitive security parameter management;
- self-tests;
- life-cycle assurance; and
- mitigation of other attacks.

The overall security rating or the security level within each area of a cryptographic module is chosen to provide a level of security which is appropriate for the security requirements of the application and environment in which the module is utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an appropriate level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, conformity with this document does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to:

- physical and environmental controls;
- access controls;
- system security maintenance and patch management;
- backup and contingency plans; and
- information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.

Conformity with this document is not sufficient to ensure that a module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

## ISO/IEC FDIS 19790:2024(en)

Owners of sensitive information are expected to assess the risks to their information and to deploy cryptographic modules as part of their overall risk mitigation plan, in order to mitigate specific identified risks. The security policy of the module, which outlines its strengths and limitations, is expected to be followed for any given deployment.

# iTeh Standards (<https://standards.itih.ai>) Document Preview

[ISO/IEC FDIS 19790](https://standards.itih.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790)

<https://standards.itih.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>





# Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

## 1 Scope

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in information and communication technologies (ICT). It defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

### 3.1 access control list

ACL

list of permissions to grant access to an object

### 3.2 administrator guidance

written material that is used by either the *crypto officer* (3.30) or any other administrative role (3.119) for the correct configuration, maintenance, and administration of the *cryptographic module* (3.35)

### 3.3 automated

without *manual* (3.81) intervention or input (e.g. electronic means such as through a computer network)

### 3.4 approved data authentication technique

approved method providing assurance that the originator of the data is as claimed

Note 1 to entry: Approved data authentication techniques can include the use of an approved *digital signature* (3.43), approved *message authentication code* (3.82) or approved keyed hash. Approved data authentication techniques are specified in Annex C.

### 3.5 approved integrity technique

approved method of verifying whether or not data has been corrupted or modified

Note 1 to entry: Approved integrity techniques can be keyed, and can include an approved hash, a *message authentication code* (3.82) or a *digital signature* (3.43) algorithm.

Note 2 to entry: Approved integrity techniques are specified in [Annex C](#).

### 3.6 approved process

set of interrelated functions that includes at least one *approved security function* ([3.8](#)), and can include a non-cryptographic function or non-approved *security function* ([3.126](#)) which are not security relevant to the process's operation

Note 1 to entry: A banking transaction, a compression service that includes encryption, etc.

### 3.7 approved service

*service* ([3.136](#)) which includes at least one *approved security function* ([3.8](#)) or process, and can include *non-security relevant* ([3.91](#)) functions or processes

Note 1 to entry: Any *security relevant* ([3.128](#)) but non-approved security functions or processes are excluded from approved services.

### 3.8 approved security function

*security function* ([3.126](#)) that is permitted for use in an *approved service* ([3.7](#))

Note 1 to entry: Approved security functions are referenced in [Annex C](#), which references [Annex D](#) and [Annex E](#).

### 3.9 asymmetric algorithm

asymmetric technique

*cryptographic algorithm* ([3.31](#)) or technique that uses two related transformations: a public transformation (defined by the *public key* ([3.113](#))) and a private transformation (defined by the *private key* ([3.110](#)))

Note 1 to entry: The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with given computational resources.

### 3.10 attestation

process used to allow an *entity* ([3.49](#)) outside the boundary of the *cryptographic module* ([3.35](#)) to securely verify the identity and other physical or logical characteristics of the cryptographic module using an *attestation record* ([3.11](#))

Note 1 to entry: An attestation conforms to the attestation standards and methods listed in [Annex G](#).

### 3.11 attestation record

record that is generated by and retrievable from a *cryptographic module* ([3.35](#)) that supports the *attester service* ([3.12](#))

Note 1 to entry: The attestation record contains measurement details about *software* ([3.140](#)), *firmware* ([3.58](#)) or *hardware* ([3.64](#)) components within the cryptographic module. Measurements can include hash values or copies of software, firmware, or hardware components within the cryptographic module as well as configuration settings, *status information* ([3.145](#)), registers, and fuse values.

### 3.12 attester service

*service* ([3.136](#)) that a *cryptographic module* ([3.35](#)) can support, which requires the module to support an identity and the generation of an *attestation record* ([3.11](#))

### 3.13 authentication data

data entered into the *cryptographic module* ([3.35](#)) by the *operator* ([3.98](#)), used to authenticate the operator to the module

Note 1 to entry: Authentication data are transient and are considered a temporary *critical security parameter* ([3.29](#)).

Note 2 to entry: During an authentication attempt, authentication data are submitted to the module as:

- a) a data input by the operator (e.g. a *password* (3.102), *personal identification number* (3.103), *cryptographic key* (3.34) or equivalent); or
- b) the result of a method/process involving operator related information (e.g. the signing of a challenge with a *private key* (3.110), insertion of a physical key, processing of *biometric* (3.15) data).

**3.14  
authorized**

when an *operator* (3.98) has authority to assume a specific *role* (3.119) and perform a corresponding set of services

**3.15  
biometric**

measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an *operator* (3.98)

**3.16  
bitstream**

series of instructions parsed by a field programmable gate array (FPGA) on start-up to configure its internal logic

Note 1 to entry: Bitstream is considered a highly customized form of executable code.

**3.17  
certificate**

data of an entity, which is rendered unforgeable with the private or secret key of a certification authority (CA)

Note 1 to entry: This term should not be confused with a module's validation certificate issued by a *certification body* (3.18).

**3.18  
certification body**

third-party conformity assessment body operating a certification scheme

Note 1 to entry: A certification body can be non-governmental or governmental (with or without regulatory authority).

Note 2 to entry: A certification body that assesses conformance to this document is known as a validation authority.

Note 3 to entry: A certification scheme is a system related to specified products, to which the same specified requirements, specific rules and procedures apply.

[SOURCE: ISO/IEC 17065:2012, 3.12]

**3.19  
compromise**

unauthorized disclosure, modification, substitution, or use of a *critical security parameter* (3.29), the unauthorized modification or substitution of a *public security parameter* (3.115), or the loss of *integrity* (3.72) or availability of the *cryptographic module* (3.35) itself, which can result in an unintended bypass of security functions supported by the module

**3.20  
conditional self-test**

test performed by a *cryptographic module* (3.35) when the conditions specified for the test occur

**3.21  
confidential**

intending that information is not made available or disclosed to unauthorized entities

### 3.22

#### **configuration management**

discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specific requirements

[SOURCE: ISO/IEC/IEEE 24765:2017 3.779.1, modified — in the definition "specified" has been replaced by "specific".]

### 3.23

#### **configuration management system**

CMS

set of procedures and tools (including their documentation) used by a *vendor* (3.156) to develop and maintain configurations of a *cryptographic module* (3.35) during its life cycle

### 3.24

#### **control information**

commands, signals (e.g. clock input/output), and control data (including function calls and *manual* (3.81) control data such as from switches, buttons, and keyboards) used to direct or control the operation of a *cryptographic module* (3.35) or disjoint components of a *hybrid module* (3.68)

### 3.25

#### **control input**

*control information* (3.24) that is input into a *cryptographic module* (3.35) or disjoint components of a *hybrid module* (3.68)

### 3.26

#### **control input interface**

*vendor* (3.156) identified interface(s) for which all *control information* (3.24) is input into the *cryptographic module* (3.35)

### 3.27

#### **control output**

*control information* (3.24) that is output from a *cryptographic module* (3.35) or disjoint component of a *hybrid module* (3.68) to be used as *control input* (3.25) into another cryptographic module or disjoint component of a hybrid module

### 3.28

#### **control output interface**

*vendor* (3.156) identified interface(s) for which all *control information* (3.24) is output from the *cryptographic module* (3.35)

### 3.29

#### **critical security parameter**

CSP

security related information whose unauthorized access, use, disclosure, modification and substitution can cause a *compromise* (3.19) of the security of a *cryptographic module* (3.35)

EXAMPLE Secret and private *cryptographic key* (3.34), *authentication data* (3.13) or *verifier data* (3.157) such as a *password* (3.102) or *personal identification number* (3.103).

Note 1 to entry: A CSP can be *plaintext* (3.105) or encrypted.

### 3.30

#### **crypto officer**

*role* (3.119) taken by an *operator* (3.98) that accesses a *cryptographic module* (3.35) in order to perform cryptographic initialization or management functions of a cryptographic module (e.g. module initialization, management of *sensitive security parameters* (3.131) and auditing)

**3.31**

**cryptographic algorithm**

well-defined computational procedure that takes variable inputs, which can include a *cryptographic key* (3.34), and produces an output

Note 1 to entry: Approved cryptographic algorithm standards are included in [Annex C](#).

**3.32**

**cryptographic boundary**

explicitly defined perimeter that establishes the boundary of all components (i.e. set of *hardware* (3.64), *software* (3.140) or *firmware* (3.58) components) of the *cryptographic module* (3.35)

**3.33**

**cryptographic bypass**

ability of a *service* (3.136) to partially or wholly circumvent a cryptographic function or process

**3.34**

**cryptographic key**

key

sequence of symbols that controls the operation of a cryptographic transformation

Note 1 to entry: A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check value computation, signature generation, or signature verification.

**3.35**

**cryptographic module**

module

set of *hardware* (3.64) and either *software* (3.140) or *firmware* (3.58) that implements security functions and are contained within the *cryptographic boundary* (3.32)

**3.36**

**cryptographic module security policy**

security policy

precise specification of the security rules under which a *cryptographic module* (3.35) will operate, including the rules derived from the requirements of this document and additional rules imposed by the module or *certification body* (3.18)

Note 1 to entry: See [Annex B](#).  
<https://standards.iteh.ai/catalog/standards/iso/74c98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>

**3.37**

**cryptographic operation**

implementation of one or more *cryptographic algorithm* (3.31) in the *cryptographic module* (3.35)

**3.38**

**data input interface**

*vendor* (3.156) identified interface(s) for which all *input data* (3.71) is input into the *cryptographic module* (3.35)

**3.39**

**data output interface**

*vendor* (3.156) identified interface(s) for which all *output data* (3.99) is output from the *cryptographic module* (3.35)

**3.40**

**data path**

physical or logical route over which data passes

Note 1 to entry: A physical data path can be shared by multiple logical data paths.

**3.41**

**debugging technique**

method used to halt or alter the execution of the *cryptographic module* (3.35) to analyse malfunctions, using interfaces or tools that can modify objects in memory (e.g. including executable code), in a way that it is possible to bypass security controls

Note 1 to entry: Security controls are considered to be any feature of the executable code required to meet the functional requirements of this document.

**3.42**

**degraded operation**

operation where a subset of the entire set of security functions, services or processes are either available or configurable or both as a result of reconfiguration from an error state

**3.43**

**digital signature**

data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and *integrity* (3.72) of the data unit and protect against forgery (e.g. by the recipient)

**3.44**

**direct entry**

entry of a *sensitive security parameter* (3.131) or *key component* (3.74) into a *cryptographic module* (3.35), using a device such as a keyboard or number pad

**3.45**

**disjoint signature**

signature used as part of a group of signatures, which together represent an entire set of code

**3.46**

**electronic entry**

entry of a *sensitive security parameter* (3.131) or *key component* (3.74) into a *cryptographic module* (3.35) using electronic methods

Note 1 to entry: It is possible that the *operator* (3.98) of the *cryptographic module* (3.35) has no knowledge of the value of the key being entered.

**3.47**

**encompassing signature**

single signature for an entire set of code

**3.48**

**encrypted critical security parameter**

encrypted CSP

*critical security parameter* (3.29) that has been encrypted using an *approved security function* (3.8)

**3.49**

**entity**

person, group, device or process

**3.50**

**entropy**

measure of the disorder, randomness or variability in a closed system

Note 1 to entry: The entropy of a random variable  $X$  is a mathematical measure of the amount of information provided by an observation of  $X$ .

**3.51**

**environmental failure protection**

EFP

use of features to protect against a *compromise* (3.19) of the security of a *cryptographic module* (3.35) due to environmental conditions outside of the module's normal operating range