

---

# Security for industrial process measurement and control —

## Part 3: Network and system security

ICS 25.040.40; 35.040; 35.110





## National foreword

This Draft for Development is the UK implementation of IEC/PAS 62443-3:2008.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

A PAS is a Technical Specification not fulfilling the requirements for a standard, but made available to the public and established in an organization operating under a given procedure.

A review of this Draft for Development will be carried out not later than three years after its publication.

Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development, will be made in an announcement in the appropriate issue of Update Standards.

According to the replies received, the responsible BSI Committee will judge whether the validity of the PAS should be extended for a further three years or what other action should be taken and pass their comments on to the relevant international committee.

Observations which it is felt should receive attention before the official call for comments will be welcomed. These should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 29 August 2008

© BSI 2008

ISBN 978 0 580 62208 3

### Amendments/corrigenda issued since publication

Date	Comments



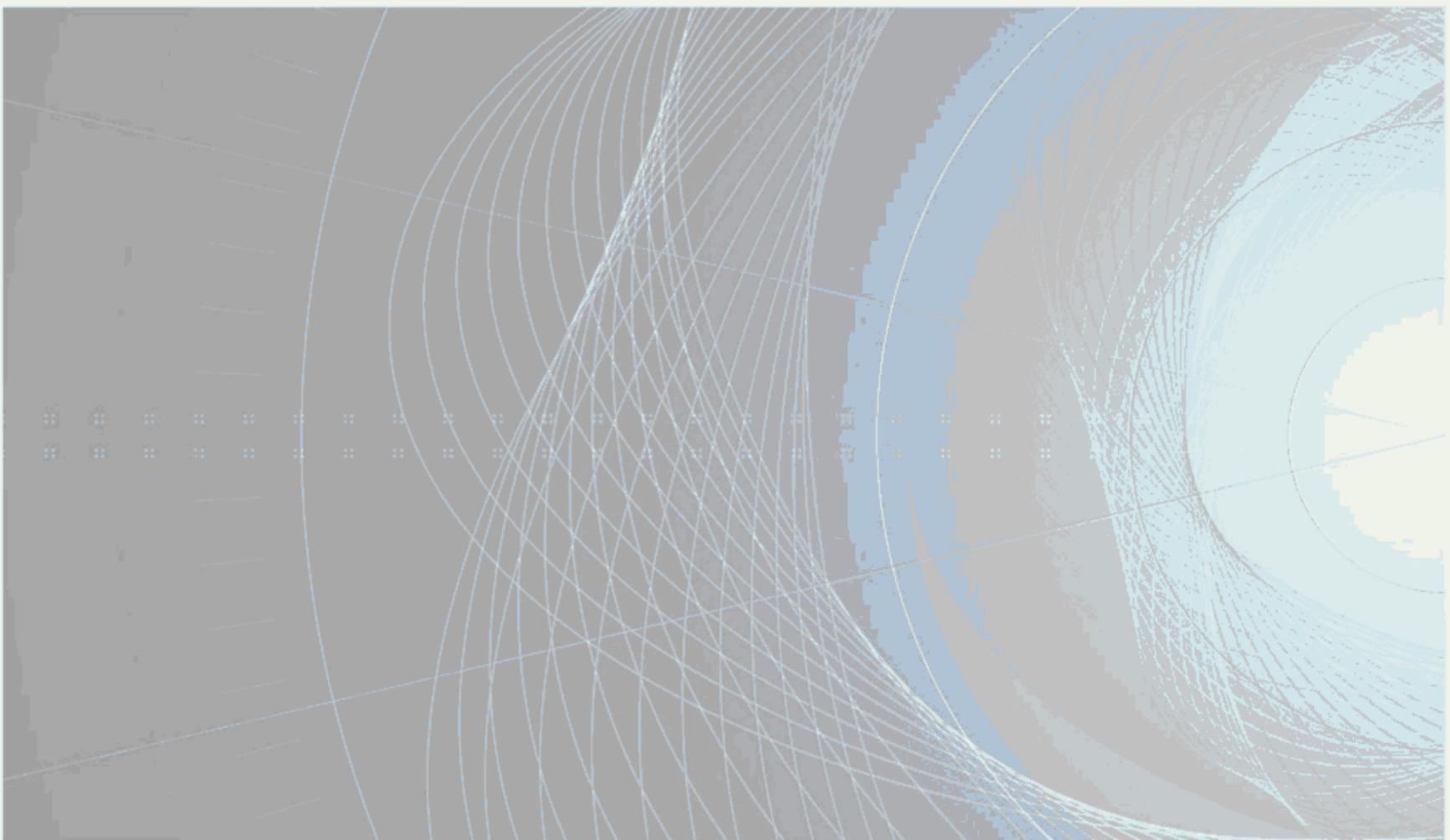
DD IEC/PAS 62443-3:2008  
**IEC/PAS 62443-3**

Edition 1.0 2008-01

# **PUBLICLY AVAILABLE SPECIFICATION PRE-STANDARD**

---

**Security for industrial process measurement and control – Network and system security**



## CONTENTS

INTRODUCTION.....	3
1 Scope.....	4
2 Normative references .....	4
3 Terms, definitions, symbols, abbreviated terms and conventions .....	5
3.1 Terms and definitions .....	5
3.2 Symbols and abbreviated terms.....	11
4 Introduction and compliance.....	12
5 Principles and reference models.....	12
5.1 General .....	12
5.2 Threat-risk model .....	13
5.3 Security life cycle .....	15
5.4 Policy .....	16
5.5 Generic reference configurations.....	19
5.6 Protection models .....	22
6 ICS security policy – Overview .....	27
7 ICS security policy – Principles and assumptions .....	29
7.1 ICS security policy – Principles .....	29
7.2 ICS security policy – Assumptions and exclusions.....	30
7.3 ICS security policy – Organization and management. ....	32
8 ICS security policy – Measures.....	36
8.1 Availability management.....	36
8.2 Integrity management.....	38
8.3 Logical access management .....	41
8.4 Physical access management.....	44
8.5 Partition management .....	45
8.6 External access management.....	46
Annex A Projected new edition of IEC 62443 .....	50
Bibliography.....	52
Figure 1 – Threat-risk relationship .....	13
Figure 2 – Security life cycle.....	15
Figure 3 – Policy levels.....	17
Figure 4 – Industrial control system (ICS) .....	20
Figure 5 – GPH reference configuration: Generic ICS host with external devices .....	21
Figure 6 – Device protection: Hardening and access management.....	22
Figure 7 – Defense-in-depth through partitioning .....	24
Figure 8 – Example: ICS partitioning.....	25
Figure 9 – Generic external connectivity .....	26

## INTRODUCTION

The increasing degree of public networking of formerly isolated automation systems increases the exposure of such systems to attack. Standard IT security protection mechanisms have protection goals and strategies that may be inappropriate for automation systems. This PAS addresses the topic of securing access to and within industrial systems while assuring timely response which may be critical to plant operation.

For safety applications and applications in the pharmaceutical or other highly specialized industries, additional standards, guidelines, definitions and stipulations may apply, for example, IEC 61508, GAMP (ISPE), for GMP Compliance 21 CFR (FDA) and the Standard Operating Procedure of the European Medicines Agency (SOP/INSP/2003).

## SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL – NETWORK AND SYSTEM SECURITY

### 1 Scope

This PAS establishes a framework for securing information and communication technology aspects of industrial process measurement and control systems including its networks and devices on those networks, during the operational phase of the plant's life cycle.

This PAS provides guidance on a plant's operational security requirements and is primarily intended for automation system owners/operators (responsible for ICS operation)

Furthermore, the operational requirements of this PAS may interest ICS stakeholders such as:

- a) automation system designers;
- b) manufacturers (vendors) of devices, subsystems, and systems;
- c) integrators of subsystems and systems.

The PAS allows for the following concerns:

- graceful migration/evolution of existing systems;
- meeting security objectives with existing COTS technologies and products;
- assurance of reliability/availability of the secured communications services;
- applicability to systems of any size and risk (scalability);
- coexistence of safety, legal and regulatory and automation functionality requirements with security requirements.

NOTE 1 Plants and systems may contain safety critical components and devices. Any safety-related security components may be subject to certification based on IEC 61508 and according to the SILs therein. This PAS does not guarantee that its specifications are all or in part appropriate or sufficient for the security of such safety critical components and devices.

NOTE 2 This PAS does not include requirements for security assurance evaluation and testing.

NOTE 3 The measures provided by this PAS are rather process-based and general in nature than technically specific or prescriptive in terms of technical countermeasures and configurations.

NOTE 4 The procedures of this PAS are written with the plant owner/operator's mind set.

NOTE 5 This PAS does not cover the concept, design and implementation live cycle processes, i.e. requirements on control equipment manufacturer's future product development cycle.

NOTE 6 This PAS does not cover the integration of components and subsystems into a system.

NOTE 7 This PAS does not cover procurement for integration into an existing system, i.e. procurement requirements for owner/operators of a plant.

NOTE 8 This PAS will be extended into a 3-part International Standard to cover most of the restrictions expressed in the previous notes; for the planned scope of the extended standards, refer to Annex A.

### 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT security*

ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for IT security management*

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

### **3 Terms, definitions, symbols, abbreviated terms and conventions**

#### **3.1 Terms and definitions**

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

##### **3.1.1**

###### **access control**

prevention of unauthorized use of a restricted resource, including its use in an unauthorized manner

[ISO/IEC 18028-2:2006, modified]

##### **3.1.2**

###### **adversary**

entity that attacks, or is a threat to, a system

[RFC 2828]

##### **3.1.3**

###### **alert**

instant indication that an information system and network may be under attack, or in danger because of accident, failure or people error

[ISO/IEC 18028-1:2006]

##### **3.1.4**

###### **asset**

anything that has value to the organization

[ISO/IEC 13335-1:2004]

##### **3.1.5**

###### **assurance**

performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives

[ISO/IEC/TR 15443-1]

##### **3.1.6**

###### **attack**

attempts to destroy, expose, alter, or disable an information system and/or information within it or otherwise reach the security policy

[ISO/IEC 18043]

##### **3.1.7**

###### **attack surface**

set of system resources exposed directly and indirectly to potential attack.

##### **3.1.8**

###### **audit**

formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

[ISO/IEC 18028-1]

##### **3.1.9**

###### **authenticate, authentication**

provision of assurance of the claimed identity of an entity

[ISO/IEC 19792]

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10  
availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11  
commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12  
compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13  
confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14  
credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15  
demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16  
denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17  
event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18  
exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19  
external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

**3.1.10****availability**

property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

**3.1.11****commercial off-the shelf (COTS)**

items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

**3.1.12****compromise**

unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

**3.1.13****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

**3.1.14****credentials**

means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

**3.1.15****demilitarized zone (DMZ)**

security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks

[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

**3.1.16****denial of service (attack)**

attack against a system to deter its availability

[ISO/IEC 18028-4]

**3.1.17****event**

occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

**3.1.18****exposed, exposure**

evident state of being vulnerable and exposed to attack

**3.1.19****external**

outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network