

PAS 7040:2019

Digital manufacturing – Trustworthiness and precision of networked sensors – Guide



Innovate UK

bsi
Documents
Document Sharing Hub

AVA

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2019.

Published by BSI Standards Limited 2019.

ISBN 978 0 539 035391

ICS 25.040.01, 35.240.50

No copying without BSI permission except as permitted by copyright law.

Publication history

First published November 2019

Contents

Foreword	ii
Introduction	iii
1 Scope	1
2 Normative references	2
3 Terms, definitions and abbreviations	3
4 Networked sensors and the needs for trustworthiness and security..	10
5 Measurement and sensor fundamentals	15
6 Provenance of sensors and their data	21
7 Assessing and managing trustworthiness and security needed	28
8 Implementing the organization's networked sensor strategy	32
9 Sensor trust, identity and trustworthiness data transmitted over a network	34
10 Sharing sensor data	35
11 Managing uncertainty	36
12 Utility, storage, maintenance and management of sensor data and information	38
Bibliography	39
List of figures	
Figure 1 – Holistic approach to security.....	12
Figure 2 – Elements typically found in a networked sensor.....	16
Figure 3 – Generic data and information lifecycle.....	20
Figure 4 – Relationship of a sensor to the data and information lifecycle	21
Figure 5 – Relationship between a sensor, measurement requirements and testing	23
Figure 6 – The sensor's lifecycle	25
Figure 7 – Risk management approach	28
List of tables	
Table 1 – International System of Units (SI)	15
Table 2 – Examples of characteristics of a sensor's measurements	18

Foreword

This PAS (Publicly Available Specification) was sponsored by Innovate UK. Its development was facilitated by BSI Standards Limited, and it was published under licence from The British Standards Institution. It came into effect on 30 November 2019.

Acknowledgement is given to Hugh Boyes, Bodvoc Limited, as the technical author, and the following organizations that were involved in the development of this PAS as members of the steering group:

- Bodvoc Limited
- Centre for the Protection of National Infrastructure
- DEX Europe Limited
- Innovate UK
- Knowledge Transfer Network
- National Physical Laboratory Limited
- Rolls-Royce plc.

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a guide to be rapidly developed to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice.

Presentational conventions

The guidance in this PAS is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Explanation and general informative material is presented in smaller italic type and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

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

Compliance with a PAS cannot confer immunity from legal obligations

Introduction

The increasing digitalization and automation of many industries has led to greater reliance on the use of sensors to provide measurements of physical attributes of manufactured items, processes and environmental conditions. Sensors form a vital part of measurement and automation applications and are useful for making in-situ measurements, for example, in industrial systems.

Sensors can have one of the following characteristics:

- safety or security critical, measuring the state of assets, processes and products in hazardous or demanding environments;
- embedded in products, systems or the environment; or
- body worn to detect conditions that may harm the health or wellbeing of operatives working in potentially hazardous environments.

For the purposes of this PAS, a sensor is defined as a device which detects, measures or identifies changes to a physical property or phenomenon and then provides a measurable response or indication.

This PAS addresses the trustworthiness of sensors and their data, taking into account measurement and sensor fundamentals, the provenance of sensors and their data and the assessment of measurement uncertainty. It examines security issues that may impact on the trustworthiness of sensors and their use, including the transmission of data over a network. A risk management process for sensors is set out as well as the need for an organization to have a strategy for the use of and reliance on networked sensors. The issue of sensor trust and identity is examined, along with measures regarding the sharing of sensor data and the maintenance of its long-term usefulness.

This page is deliberately left blank.

1 Scope

This PAS gives guidance on the quality and security plans for measurements generated by network sensors and transmitted over a network, in a manufacturing production line, or associated servitization. It includes guidance on how to assure measurements and support the process of adoption within key industry stakeholders.

It covers:

- a) determining the need for a sensor, or sensors, and assessing the functional and non-functional requirements (i.e. the physical need and informational aspects are understood);
- b) precision of sensor measurements in a production environment for a standard set of metrics delivered in a secure network;
- c) identification of sensor entities and associated measurements;
- d) origin of the data transmitted and received in a production environment;
- e) relationship with internet of things (IoT)/industrial internet of things (IIoT) catalogues;
- f) security of Internet communication between a sensor and dependent components within a protected firewall/secure network (barrier to cyber-attack);
- g) methods for mitigating operational ambiguity and security threats to data, information, physical components, technical systems, and associated processes that might affect the people who use (directly or indirectly, work with, handle, or are nearby) products that rely upon measurements from sensors;
- h) measures to handle the normal operational tolerances of sensors, as well as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities that are directly associated with such measurements;

- i) technological aspects including safety, authenticity, availability (including reliability), confidentiality, integrity, possession, resilience and utility (including precision/accuracy); and
- j) accuracy and authenticity of calibration of sensors, over a secure Internet /intranet.

It does not cover:

- 1) independent validation of measurement assurance;
- 2) sensing outside of a manufacturing or a process control sector.

The target audience for this PAS is organizations that design, build, sell and maintain networked sensors for digital manufacturing applications and that acquire, integrate and maintain them in operational deployments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document.¹⁾ For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

PAS 1085:2018, *Manufacturing – Establishing and implementing a security-minded approach – Specification*

¹⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

3 Terms, definitions and abbreviations

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

3.1 Terms and definitions

3.1.1 aggregation

collection and/or collation of data and/or information through manual or automated processes thus enabling analysis that may allow meaningful and useful interpretation of initially isolated or independent facts or data

NOTE 1 Aggregation has the potential to increase the business impact of any compromise, whether accidental or intentional.

NOTE 2 Data aggregation risks can arise from:

- a) aggregation by accumulation, where the volume of data and/or information stored together increases the level of impact that would occur if it was compromised;
- b) aggregation by association, where the association of different types of data and/or information, which in themselves have little or no impact when compromised, when associated together, have a higher level of impact;
- c) a combination of accumulation and association; or
- d) disclosure of too much data and/or information, e.g. in response to a public access request or media enquiry, allowing a third-party to draw inferences from the disclosed material or create unplanned associations.

3.1.2 asset

item, thing or entity that has potential or actual value to an organization

[SOURCE: BS ISO 55000:2014, 3.2.1]

NOTE 1 An asset can be fixed, mobile or movable. It can be an individual item, plant, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets.

NOTE 2 An asset might also comprise data, information in digital or in printed form, as well as an organization's internal processes.

NOTE 3 Digital information can be localized (i.e. based on a single data source) or distributed (i.e. derived from multiple data sources and/or locations).

NOTE 4 The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial and non-financial.

NOTE 5 ISO 20924 defines asset as – “physical entity of digital entity that has value to an individual, an organization or a government”.

3.1.3 calibration

comparison of measurement values delivered by a sensor under test with those of a calibration standard of known accuracy

NOTE 1 The calibration standard may be another measurement device of known accuracy, a device generating the quantity to be measured or a physical artefact.

NOTE 2 A calibration standard may be traceable to a national standard held by a National Metrological Institute, which in the UK is the National Physical Laboratory (NPL).

3.1.4 change management

systematic processes and procedures used to manage changes to assets that may affect the assets performance, functional, and physical attributes or require variations to its functional and non-functional requirements, design, and operational information

NOTE 1 The process typically encompasses submission of a change proposal documenting the proposed changes, a review stage for stakeholders to assess the proposed change and its impact on the asset and related business operations, and an approval, reject or resubmission stage, such that only approved changes are authorized for implementation.

NOTE 2 Where a change to an asset is approved and implemented the relevant configuration management records may be updated to reflect the changes to the asset.

NOTE 3 Change management for industrial automation systems is addressed in ISO 18828-5.

3.1.5 configuration management

engineering process for establishing and maintaining the consistency of an asset in respect of its performance, functional, and physical attributes with its functional and non-functional requirements, design, and operational information throughout the asset's life

NOTE For individual assets the configuration information may remain largely unchanged through, however it may be updated whenever an asset is maintained or calibrated to maintain the service and calibration history for the asset.

3.1.6 context

circumstances that form the setting for an asset, event, data and/or information, which allow its significance and/or meaning to be better understood

[SOURCE: PAS 1085:2018, 3.1.4]

NOTE From a trustworthiness perspective the environmental context is important, i.e. what environment is the sensor being deployed and therefore what associated environmental and physical protection is required. For example, the environment will influence the choice of IP rating required for the sensor, power source, controls data cables etc., and the physical protection and/or anti-tampering measures required. If wireless connectivity is employed to connect the sensor to the network, the context includes the RF and EMI environments.

3.1.7 data

series of digital or analogue signals or encoded characters stored or transmitted electronically, or marks (e.g. writing, printed characters or graphics) on paper or microform, that are intended to convey information

[SOURCE: BIP 0008-1]

NOTE The essential distinction between data and information is that data doesn't need to have any meaning attached to it. Data becomes information via context; this means, the same data file may be considered as containing different information depending on the context. For example, one computer programme can assess the data in the same file as containing ASCII characters, another can regard the same data as a set of names and addresses, i.e. the user can know that these are customer names and addresses.

3.1.8 data sharing

provision of data from one or more organizations to a third-party organization or organizations, reciprocal exchange of data between organizations, or sharing of data between different parts and/or systems of the same organization

{SOURCE: ICO's Data Sharing Code of Practice [7], modified}

NOTE 1 There are two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared between the same organizations, or parts of an organization, for an established purpose; and
- exceptional, one-off decisions to share data, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.

NOTE 2 Data sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

3.1.9 data and information sharing agreement (DISA)

set of rules to be adopted by the various organizations involved in a data and/or information sharing operation

[SOURCE: PAS 1085:2018, 3.1.9]

3.1.10 disclosure

action of making sensitive, classified or private data and/or information known

[SOURCE: PAS 1085:2018, 3.1.10]

3.1.11 hostile reconnaissance

activity of acquiring information about a target with the view to planning to attack, compromise, disrupt or destroy that target

[SOURCE: PAS 1085:2018, 3.1.11]

NOTE 1 The target might be an individual, organization, enterprise or built asset, in whole or in part.

NOTE 2 The planned hostile action might be physical or cyber in nature.

NOTE 3 Reputational damage might result from such physical or cyber hostile actions.

3.1.12 information

data interpreted in an application context (see also 3.4)

NOTE For example, a string of characters can be referred to generally as data; but if these characters are understood by a person or a computer programme as someone's name, then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen, or the contents of an electronic file.

[SOURCE: BIP 0008-1]

3.1.13 information management

policies, processes, procedures and tasks applied to the data and/or information across its lifecycle to ensure its accuracy, authenticity, confidentiality, integrity and utility

[SOURCE: PAS 1085:201, 3.1.16]

NOTE *The information lifecycle for production systems is addressed in the ISO 18828 set of standards. ISO 18828-1 provides an overview of the standardized procedures.*

3.1.14 measurand

quantity intended to be measured

[SOURCE: JCGM 200:2012(E/F), 2.3 modified]

NOTE 1 *The specification of a measurand requires knowledge of the kind of quantity, description of the state of the phenomenon, body, or substance carrying the quantity, including any relevant component, and the chemical entities involved.*

NOTE 2 *The term measurand is sometimes defined as the “particular quantity subject to measurement”.*

NOTE 3 *The measurement, including the measuring system and the conditions under which the measurement is carried out, might change the phenomenon, body, or substance such that the quantity being measured may differ from the measurand as defined. In this case, adequate correction is necessary.*

3.1.15 measurement

process of experimentally obtaining one or more quantity values that can reasonably be attributed to a quantity

[SOURCE: JCGM 200:2012(E/F), 2.1]

NOTE 1 *Measurement does not apply to nominal properties.*

NOTE 2 *Measurement implies comparison of quantities or counting of entities.*

NOTE 3 *Measurement presupposes a description of the quantity commensurate with the intended use of a measurement result, a measurement procedure, and a calibrated measuring system operating according to the specified measurement procedure, including the measurement conditions.*

3.1.16 measurement process

set of operations to determine the value of a quantity

[SOURCE: BS EN ISO 10012:2003 3.2]

3.1.17 measuring equipment

measuring instrument, software, measurement standard, reference material or auxiliary apparatus, or a combination thereof, necessary to realize a measurement process

[SOURCE: BS EN ISO 10012:2003 3.3]

3.1.18 metrological characteristic

distinguishing feature which can influence the results of measurement

[SOURCE: BS EN ISO 10012:2003 3.4]

NOTE 1 *Measuring equipment usually has several metrological characteristics.*

NOTE 2 *Metrological characteristics can be the subject of calibration.*

3.1.19 metrological confirmation

set of operations required to ensure that measuring equipment conforms to the requirements for its intended use

[SOURCE: BS EN ISO 10012:2003 3.5]

NOTE 1 *Metrological confirmation generally includes calibration and verification, any necessary adjustment or repair, and subsequent recalibration, comparison with the metrological requirements for the intended use of the equipment, as well as any required sealing and labelling.*

NOTE 2 *Metrological confirmation is not achieved until and unless the fitness of the measuring equipment for the intended use has been demonstrated and documented.*

NOTE 3 *The requirements for intended use include such considerations as range, resolution and maximum permissible errors.*

NOTE 4 *Metrological requirements are usually distinct from, and are not specified in, product requirements.*

NOTE 5 *A metrological confirmation is illustrated in Figure 2 of BS EN ISO 10012:2003.*

3.1.20 pattern-of-life

identification of habits, routines and preferences of individual(s) or group(s) that enable prediction of future actions and/or behaviour

[SOURCE: PAS 185:2017, 3.1.31, modified]

3.1.21 pattern-of-use

identification of routine actions in the handling, operation and management of assets

[SOURCE: PAS 185:2017, 3.1.32]

NOTE *The pattern-of-use of assets could facilitate malicious pattern-of-life analysis by increasing the number of data and information sources that can be combined.*

3.1.22 personal data

information relating to an identified or identifiable living individual

{SOURCE: Data Protection Act 2018 [5], Section 1(2)}

3.1.23 personnel

individual(s) employed by an organization, including contractors or temporary staff used to fulfil roles that are undertaken by that organization

[SOURCE: PAS 1085:2018, 3.1.22]

3.1.24 personnel security

system of policies, processes and procedures that seek to mitigate the risk of workers (inside an organization) exploiting their legitimate access to that organization's assets for unauthorized purposes

[SOURCE: PAS 1085:2018, 3.1.23]

NOTE *These measures might be applied to all personnel that have access to, or use, the asset over its lifecycle, including personnel employed within the supply chain used to design, create, operate, decommission or dispose of the asset.*

3.1.25 physical security

multi-layering of different physical measures designed to deter, detect or delay an attack

[SOURCE: PAS 1085:2018, 3.1.24]

3.1.26 processing

operation or set of operations which is performed on information, or on sets of information, such as:

- a) collection, recording, organization, structuring or storage;
- b) adaptation or alteration;
- c) retrieval, consultation or use;
- d) disclosure by transmission, dissemination or otherwise making available;
- e) alignment or combination; or
- f) restriction, erasure or destruction.

{SOURCE: Data Protection Act 2018 [5], Section 1(4)}

3.1.27 referential master data

set of permissible values to be used by other data fields in shared data and/or shared information sets

[SOURCE: PAS 1085:2018, 3.1.26]

NOTE *Shared data is data that is subject to formal or informal data sharing. Shared information is information that is subject to formal or informal information sharing (see Clause 10).*

3.1.28 risk appetite

amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives

{SOURCE: Chartered Institute of Internal Auditors [1]}

NOTE 1 *Risk appetite might be set in relation to the organization, for different groups of risks, or at an individual risk level.*

NOTE 2 *In the manufacturing context, when determining the risk appetite, the needs and perspectives of all the organizations involved should be taken into account.*

3.1.29 risk capacity

resource(s), including financial, intangible and human, which an organization is able to deploy in managing risk

{SOURCE: Chartered Institute of Internal Auditors [1]}

NOTE *The organization's risk capacity is generally wider in scope than the risk appetite of the organization as it represents the limits beyond which the organization could not cope if the risk(s) occur(s). For example, when seeking insurance cover, the organization assesses what residual risk it is prepared to accept, i.e. its risk appetite which might be reflected in the excess payable if an insured event occurs, whilst the level of cover purchased reflects the risk capacity in respect of the insured risk(s). In assessing its risk appetite and risk capacity an organization considers both the gross risk and residual risk exposures, its reliance on controls and other mitigations, and the cost of implementing them in comparison to the consequences of the risk materializing.*

3.1.30 risk universe

full range of risks which could impact, either positively or negatively, on the ability of the organization to achieve its long-term aims

{SOURCE: Chartered Institute of Internal Auditors [1]}

3.1.31 sabotage

deliberate, malicious action carried out with the aim of weakening, obstructing, disrupting, damaging or destroying an asset, activity, service, organization or other entity

[SOURCE: PAS 1085:2018, 3.1.31]

NOTE Sabotage might also be conducted with the aim of enabling the targeting of a secondary event that occurs because of the original action for example, the evacuation of a building arising from the sabotage of a fire alarm.

3.1.32 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts, including sabotage

{SOURCE: Engineering Council, 2016 [3]}

3.1.33 security incident

event or events during which the security of an asset, organization or person is, or might be, compromised, either accidentally or deliberately

[SOURCE: PAS 1085:2018, 3.1.33 modified]

NOTE 1 Security incidents can take several forms including:

- a) unauthorized harmful modification to, damage to or destruction of a physical asset;
- b) supply of counterfeit raw materials, ingredients, physical and/or digital components, assemblies or sub-systems;
- c) loss or theft of documents, storage media, IT equipment, attractive or valuable items;
- d) loss, theft or unauthorized access to information or data;
- e) loss, compromise, unauthorized manipulation or change of project or asset information;
- f) unauthorized access to the built asset, or a restricted access area within the built asset;
- g) loss of keys, access control tokens, passes, etc.;
- h) planting of bugs or other surveillance devices; and
- i) unauthorized access to, misuse of, or fraudulent use of ICT equipment or systems.

NOTE 2 A near-miss is an event in which a security incident is narrowly avoided either accidentally or through deliberate action.

NOTE 3 In the event of a security incident there may be specific legal and regulatory requirements relating to the disclosure and reporting of the incident.

3.1.34 security-minded

understanding and routine application of appropriate and proportionate security measures in any business situation to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities and reduce the risk of security incidents

[SOURCE: PAS 1085:2018, 3.1.34]

3.1.35 sensitive data

data, the loss, misuse or modification of which, or unauthorized access to, could adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the data

[SOURCE: PAS 1085:2018, 3.1.35]

3.1.36 sensitive information

information, the loss, misuse or modification of which, or unauthorized access to, could adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information

[SOURCE: PAS 1085:2018, 3.1.36, modified]

3.1.37 sensitive personal data

personal data consisting of information as to:

- a) racial or ethnic origin of the data subject;
- b) his political opinions;
- c) his religious beliefs or other beliefs of a similar nature; and
- d) whether he is a member of a trade union.

{SOURCE: Data Protection Act 1998 [4], Section 2}

NOTE 1 Within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992 [6].

- a) his physical or mental health or condition;
- b) his sexual life;
- c) the commission or alleged commission by him of any offence; or
- d) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

NOTE 2 Sensitive personal data under the DPA [5] is defined as special categories of personal data under GDPR [12] and extends the range of personal data within this category. Under Article 9, the definition encompasses data which reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”. This definition came into force from 25 May 2018.

3.1.38 service

work done to meet some administrative, general, or user or customer need

[SOURCE: PAS 1085:2018, 3.1.38]

NOTE 1 Within the manufacturing context, a system supplying a user or customer need includes logistics, communications, utilities and product or system support.

NOTE 2 ISO 20924 defines service as distinct part of the functionality that is provided by an entity through interfaces.

3.1.39 stakeholder

third parties such as persons, personnel, or organizations that have a legitimate interest in the organization’s manufacturing activities, and/or the products, systems and any related services it delivers

NOTE 1 The reference to persons encompasses people affected by the manufacturing operations, customers of the manufacturer, and any users or people affected by use of the manufacturer’s products, systems and any related services.

[SOURCE: PAS 1085:2018, 3.1.39]

NOTE 2 ISO 20924 defines stakeholder as Individual, team, organization or classes thereof, having an interest in a system.

3.1.40 servitization

delivery of an integrated product, system or service that adds value

NOTE 1 The integrated offering may be delivered on a pay by use or other subscription model allowing the user organization to reduce capital expenditure and align operating costs with the actual use of the product or system.

NOTE 2 The service offered as part of the integrated offering may be outcome related for example guaranteeing the performance and availability of the product or system in use.

NOTE 3 The manufacturer, or service provider, may embed a variety of sensors in a servitized product or system to provide telemetry data regarding its operation and performance, e.g. to enable predictive maintenance based on measurand related to the known causes of breakdowns or systems failures.

3.1.41 system

group of interacting, interrelated, or interdependent elements forming a complex whole

[SOURCE: PAS 1085:2018, 3.1.42]

NOTE A system can include physical, digital, process and human elements.

3.1.42 telemetry data

data delivered by automated measurement and communications processes, by which measurands and other data are collected at remote or inaccessible locations and transmitted to receiving equipment for monitoring and analysis

3.1.43 threat

potential cause of an incident which might result in harm to an asset(s), individual(s), and/or organization(s)

[SOURCE: PAS 1085:2018, 3.1.43]

3.1.44 trustworthy

appropriately addresses safety, reliability, availability, resilience and security issues

[SOURCE: BS 10754:2018, 3.29]

NOTE 1 ISO 20924 defines trustworthiness as property of deserving trust or confidence.

NOTE 2 ISO 20924 defines IoT trustworthiness as property of deserving trust or confidence within the entire lifecycle of an Internet of Things implementation to ensure security, privacy, safety, reliability and resilience.

3.1.45 validation

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[SOURCE: BS EN ISO/IEC 27043:2016, 3.16]

3.1.46 verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[SOURCE: BS EN ISO/IEC 27043:2016, 3.17]

3.1.47 vulnerability

weakness that can be exploited by one or more threats

[SOURCE: PAS 1085:2018, 3.1.45]

3.2 Abbreviations

For the purposes of this PAS the following abbreviations apply.

DPA	Data Protection Act
EMI	Electromagnetic Interference
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control Systems
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IT/OT	Information Technology/Operational Technology
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NIS	Network and Information Systems
PFMEA	Process Failure Mode Effects Analysis
PID	Photoionization Detector
RF	Radio Frequency