PAS 7040:2019

Digital manufacturing – Trustworthiness and precision of networked sensors – Guide

Innovate UK

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2019.

ISBN 978 0 539 035391

ICS 25.040.01, 35.240.50

Publication history

First published November 2019

Contents

List of figures

List of tables

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.

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 It will be withdrawn upon publication of its content in, or as, a British Standard.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This publication can be withdrawn, revised, partially superseded or superseded.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 characeristics:

- safety or security critical, measuring the state of assets, processes and producs 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 enviornments.

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.

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.