Security for industrial automation and control systems - Part 4-1: Secure Product Development Lifecycle Requirements

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN IEC 62443-4-1:2018 sisaldab Euroopa standardi EN IEC 62443-4-1:2018 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 62443-4-1:2018 consists of the English text of the European standard EN IEC 62443-4-1:2018.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 23.03.2018.	Date of Availability of the European standard is 23.03.2018.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 25.040.40, 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62443-4-1

March 2018

ICS 25.040.40; 35.030

English Version

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements (IEC 62443-4-1:2018)

To be completed
(IEC 62443-4-1:2018)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
(IEC 62443-4-1:2018)

This European Standard was approved by CENELEC on 2018-02-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN IEC 62443-4-1:2018 E

European foreword

The text of document 65/685/FDIS, future edition 1 of IEC 62443-4-1, prepared by IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-4-1:2018.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2018-11-19
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2021-02-19

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62443-4-1:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62740	NOTE	Harmonized as EN 62470.
IEC 61508 (series)	NOTE	Harmonized as EN 61508 (series).
ISO/IEC 27001	NOTE	Harmonized as EN ISO/IEC 27001.
ISO/IEC 27002	NOTE	Harmonized as EN ISO/IEC 27002.
ISO 9001	NOTE	Harmonized as EN ISO 9001.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 62443-2-4	2015	Security for industrial process measurement and control - Network and system security - Part 2-4: Certification of IACS supplier security policies and practices	-	-
+ A1	2017		-	-

CONTENTS

INTRODUCTION

This document is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). This document describes product development life-cycle requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This document has been developed in large part from the Secure Development Life-cycle Assessment (SDLA) Certification Requirements [26] [1] from the ISA Security Compliance Institute (ISCI). Note that the SDLA procedure was based on the following sources:

– ISO/IEC 15408-3 (Common Criteria) [18];

– Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];

– The Security Development Life-cycle by Michael Howard and Steve Lipner [43];

– IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems [24], and

– RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

Therefore, all these sources can be considered contributing sources to this document.

This document is the part of the IEC 62443 series that contains security requirements for developers of any automation and control products where security is a concern.

Figure 1 illustrates the relationship of the different parts of IEC 62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

[1] Figures in square brackets refer to the bibliography.

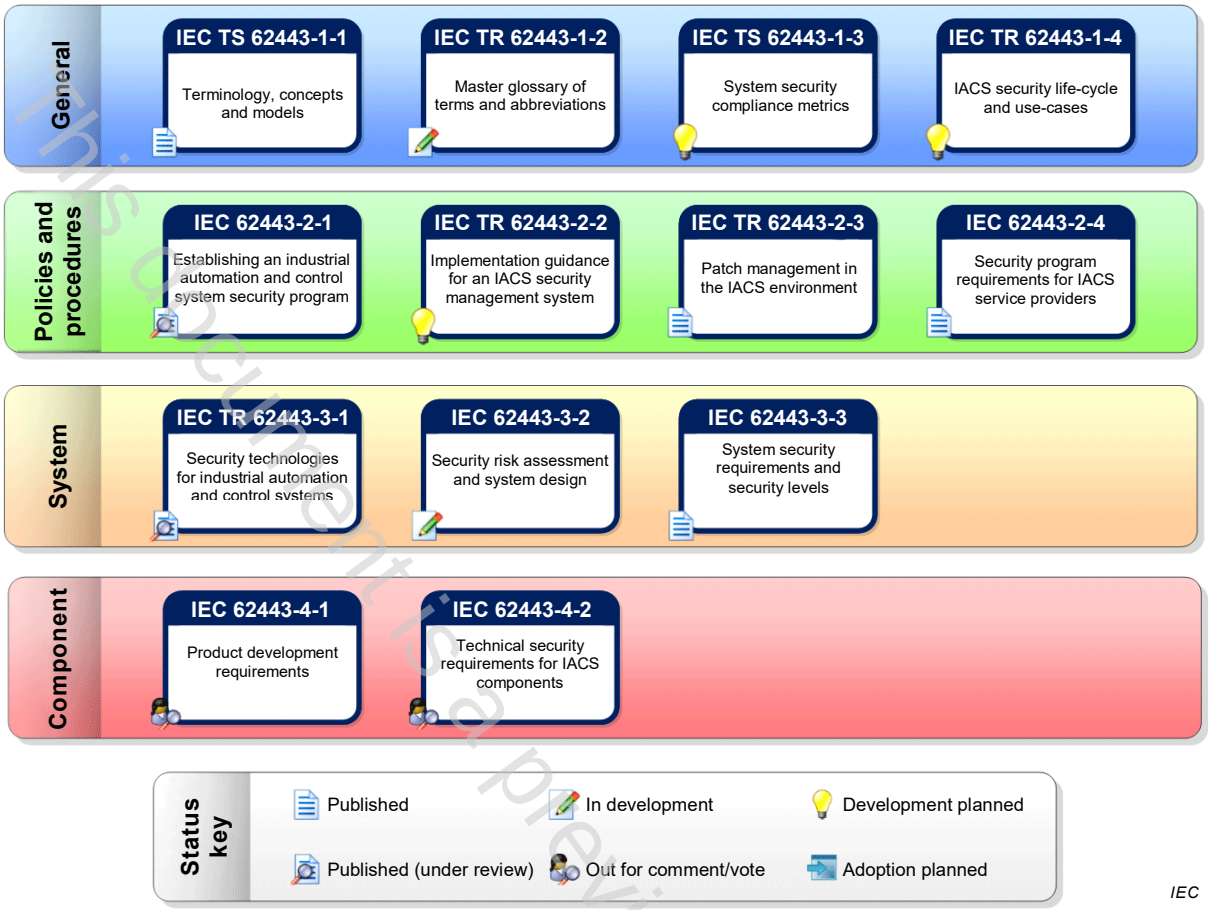

Figure 1 – Parts of the IEC 62443 series

Figure 2 illustrates how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 and to its operation by the asset owner. The product supplier develops products using a process compliant with this document. Those products may be a single component, such as an embedded controller, or a group of components working together as a system or subsystem. The products are then integrated together, usually by a system integrator, into an Automation Solution using a process compliant with IEC 62443-2-4. The Automation Solution is then installed at a particular site and becomes part of the industrial automation and control system (IACS). Some of these capabilities reference security measures defined in IEC 62443-3-3 [10] that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms). This document only addresses the process used for the development of the product; it does not address design, installation or operation of the Automation Solution or IACS.

In Figure 2, the Automation Solution is illustrated to contain one or more subsystems and optional supporting components such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 1 Automation Solutions typically have a single product, but they are not restricted to do so. In some industries, there may be a hierarchical product structure. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner.

NOTE 2 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

NOTE 3 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

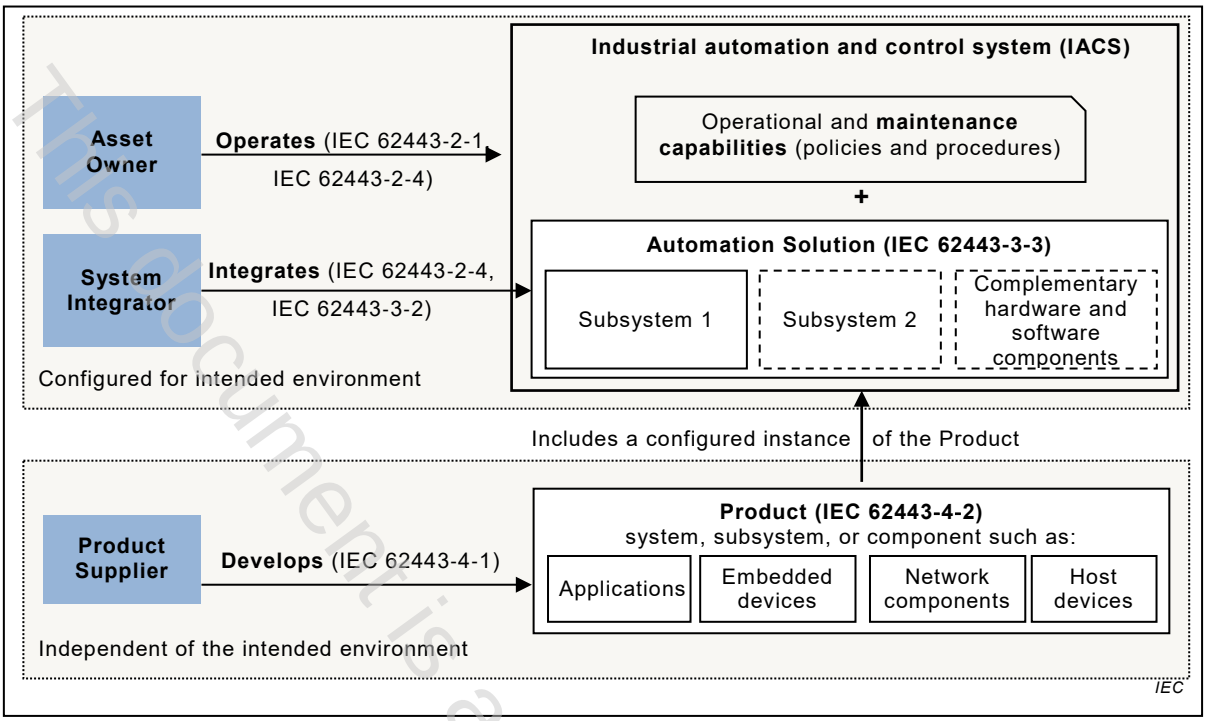

Figure 2 – Example scope of product life-cycle