

This is a preview - click here to buy the full publication



IEC 62443-2-4

Edition 1.1 2017-08
CONSOLIDATED VERSION

INTERNATIONAL STANDARD



**Security for industrial automation and control systems –
Part 2-4: Security program requirements for IACS service providers**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.110

ISBN 978-2-8322-4679-5

Warning! Make sure that you obtained this publication from an authorized distributor.

REDLINE VERSION



Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers



CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	7
3 Terms, definitions, abbreviated terms and acronyms	7
3.1 Terms and definitions.....	7
3.2 Abbreviations.....	10
4 Concepts	11
4.1 Use of IEC 62443-2-4	11
4.1.1 Use of IEC 62443-2-4 by IACS service providers	11
4.1.2 Use of IEC 62443-2-4 by IACS asset owners	12
4.1.3 Use of IEC 62443-2-4 during negotiations between IACS asset owners and IACS service providers	12
4.1.4 Profiles	13
4.1.5 IACS integration service providers	13
4.1.6 IACS maintenance service providers	14
4.2 Maturity model	14
5 Requirements overview	16
5.1 Contents	16
5.2 Sorting and filtering.....	16
5.3 IEC 62264-1 hierarchy model.....	16
5.4 Requirements table columns	16
5.5 Column definitions	17
5.5.1 Req ID column.....	17
5.5.2 BR/RE column.....	17
5.5.3 Functional area column	18
5.5.4 Topic column	19
5.5.5 Subtopic column	20
5.5.6 Documentation column	22
5.5.7 Requirement description column.....	22
5.5.8 Rationale column.....	22
Annex A (normative) Security requirements	23
Bibliography.....	90
Figure 1 – Parts of the IEC 62443 Series	5
Figure 2 – Scope of service provider capabilities	6
Table 1 – Maturity levels.....	15
Table 2 – Columns.....	17
Table 3 – Functional area column values	19
Table 4 – Topic column values.....	20
Table 5 – Subtopic column values.....	21
Table A.1 – Security program requirements	23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62443-2-4 edition 1.1 contains the first edition (2015-06) [documents 65/545/CDV and 65/561A/RVC] and its corrigendum 1 (2015-08), and its amendment 1 (2017-08) [documents 65/637A/CDV and 65/661/RVC].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 62443-2-4 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This publication contains an attached file in the form of an Excel 97-2003 spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

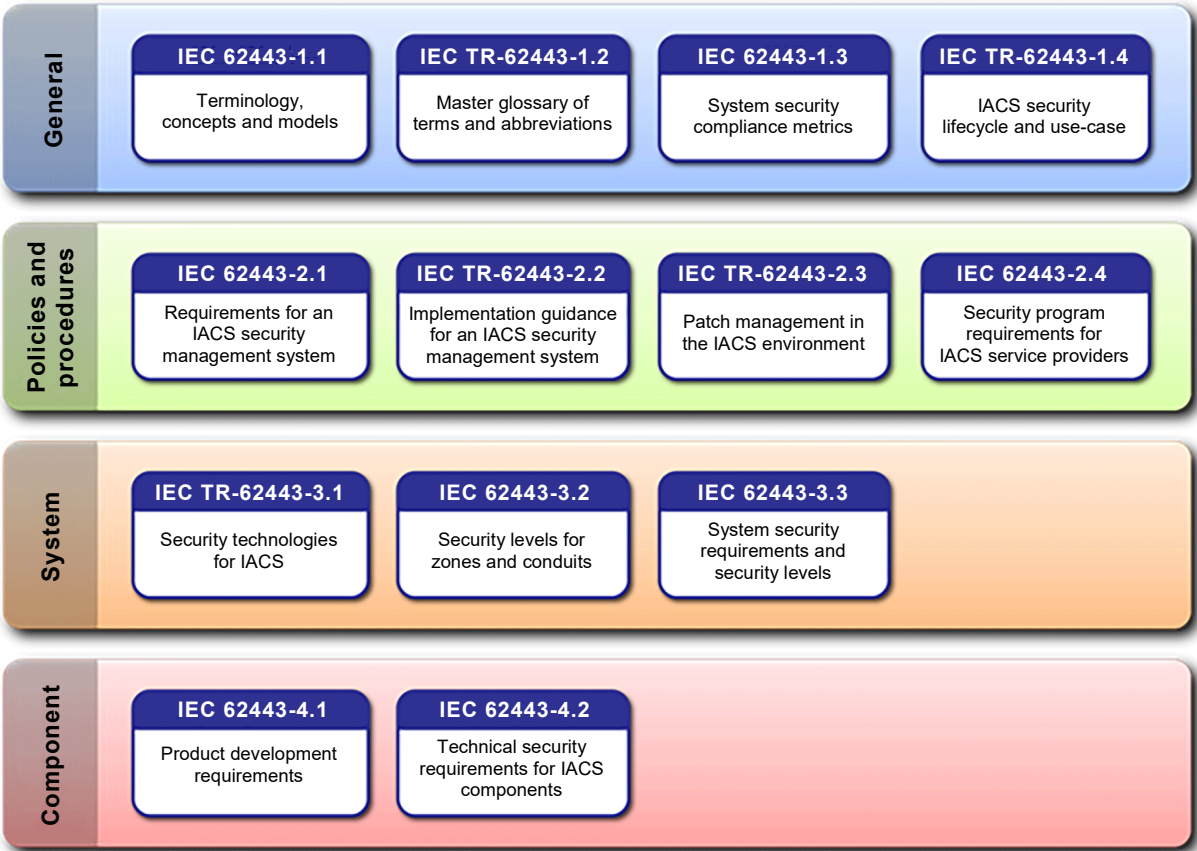
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS). It has been developed by IEC Technical Committee 65 in collaboration with the International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name, and ISA 99 committee members.

Figure 1 illustrates the relationship of the different parts of IEC 62443 being developed. 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.



IEC

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

1 Scope

This part of IEC 62443-2-4 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of Profiles that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 2 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

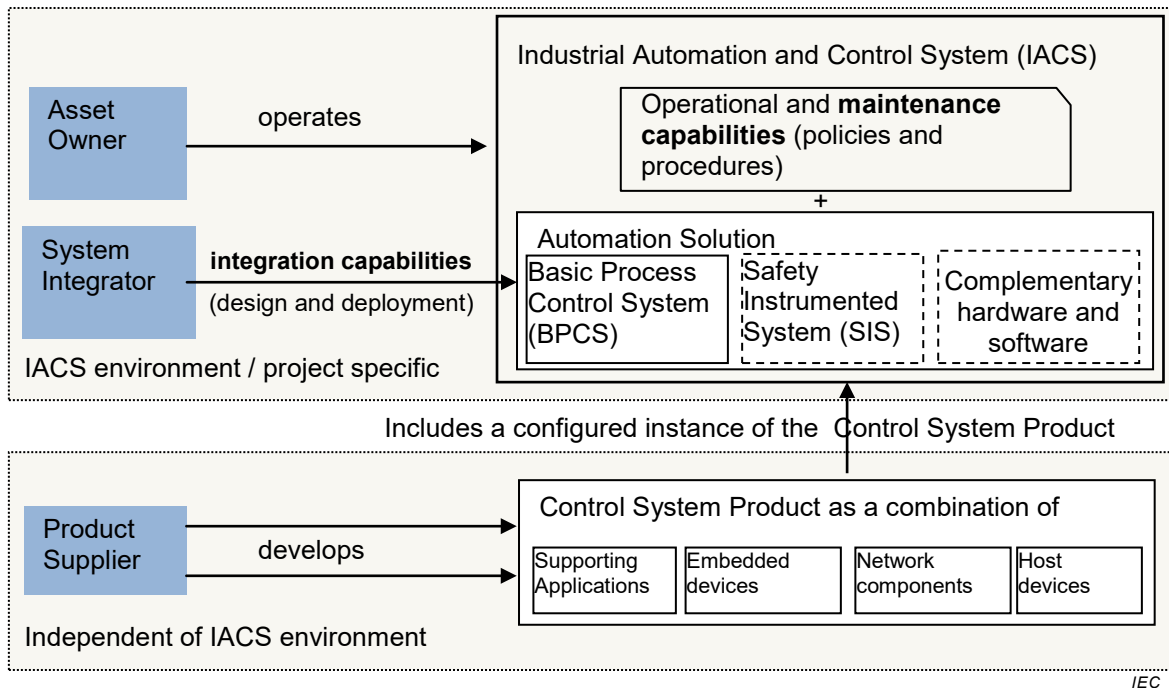


Figure 2 – Scope of service provider capabilities

IEC 62443-2-4:2015+AMD1:2017 CSV – 7 –
© IEC 2017

In Figure 2, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 3 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

~~NOTE 4—Clause 4.1.4 describes profiles and how they can be used by industry groups and other organizations to adapt this International Standard to their specific environments, including environments not based on an IACS.~~

~~NOTE 5~~ 4 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

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.

“None”



FINAL VERSION



Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers



CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	7
3 Terms, definitions, abbreviated terms and acronyms	7
3.1 Terms and definitions.....	7
3.2 Abbreviations.....	10
4 Concepts	11
4.1 Use of IEC 62443-2-4	11
4.1.1 Use of IEC 62443-2-4 by IACS service providers	11
4.1.2 Use of IEC 62443-2-4 by IACS asset owners	12
4.1.3 Use of IEC 62443-2-4 during negotiations between IACS asset owners and IACS service providers	12
4.1.4 Profiles	13
4.1.5 IACS integration service providers	13
4.1.6 IACS maintenance service providers	14
4.2 Maturity model	14
5 Requirements overview	16
5.1 Contents	16
5.2 Sorting and filtering.....	16
5.3 IEC 62264-1 hierarchy model.....	16
5.4 Requirements table columns	16
5.5 Column definitions	17
5.5.1 Req ID column.....	17
5.5.2 BR/RE column	17
5.5.3 Functional area column	18
5.5.4 Topic column	19
5.5.5 Subtopic column	20
5.5.6 Documentation column	22
5.5.7 Requirement description column.....	22
5.5.8 Rationale column.....	22
Annex A (normative) Security requirements	23
Bibliography.....	88
Figure 1 – Parts of the IEC 62443 Series	5
Figure 2 – Scope of service provider capabilities	6
Table 1 – Maturity levels.....	15
Table 2 – Columns.....	17
Table 3 – Functional area column values	19
Table 4 – Topic column values.....	20
Table 5 – Subtopic column values.....	21
Table A.1 – Security program requirements	23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SECURITY FOR INDUSTRIAL AUTOMATION
AND CONTROL SYSTEMS –**

**Part 2-4: Security program requirements
for IACS service providers**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62443-2-4 edition 1.1 contains the first edition (2015-06) [documents 65/545/CDV and 65/561A/RVC] and its corrigendum 1 (2015-08), and its amendment 1 (2017-08) [documents 65/637A/CDV and 65/661/RVC].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 62443-2-4 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This publication contains an attached file in the form of an Excel 97-2003 spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

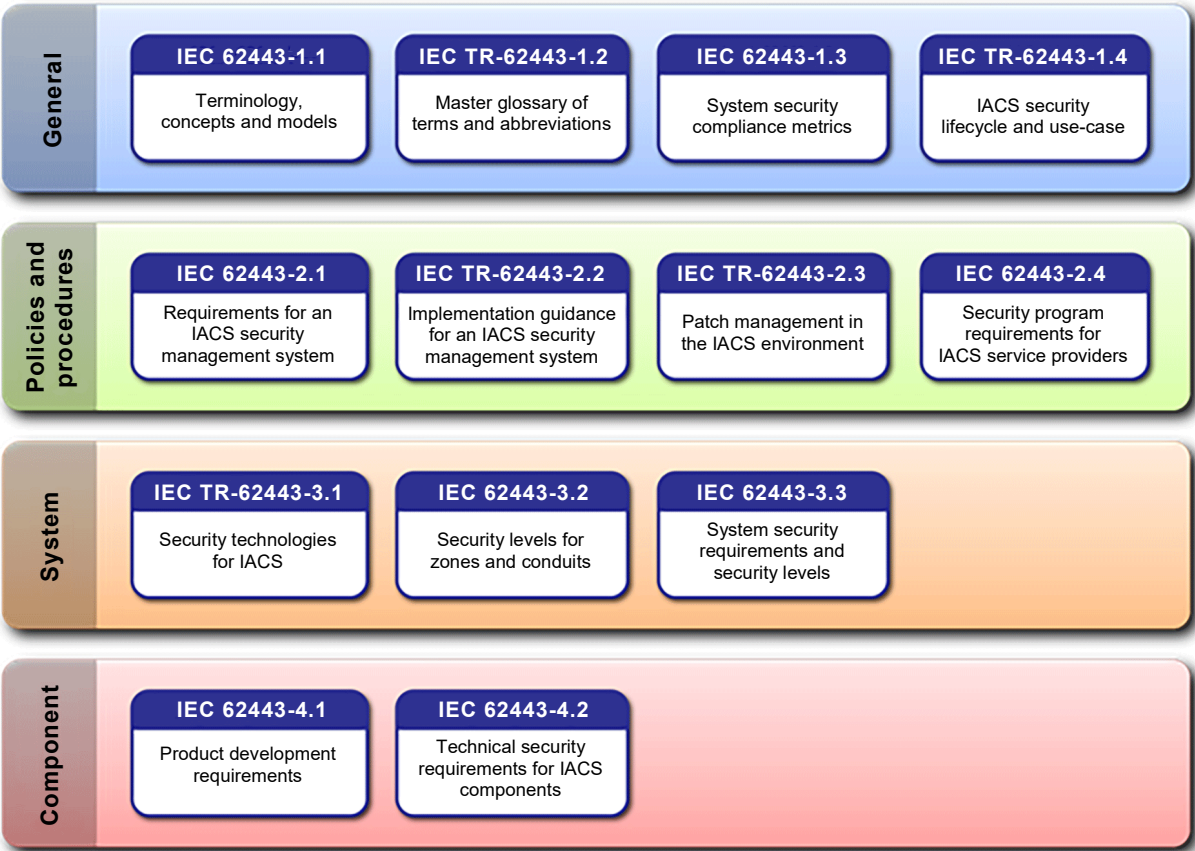
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS). It has been developed by IEC Technical Committee 65 in collaboration with the International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name, and ISA 99 committee members.

Figure 1 illustrates the relationship of the different parts of IEC 62443 being developed. 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.



IEC

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

1 Scope

This part of IEC 62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of Profiles that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 2 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

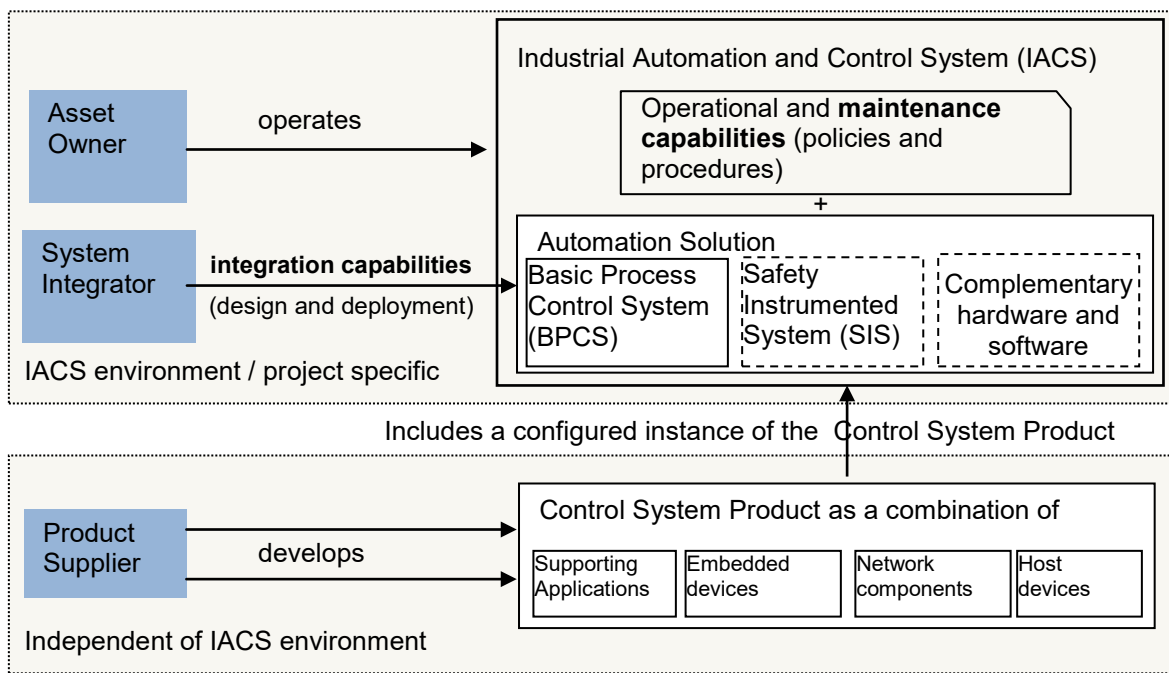


Figure 2 – Scope of service provider capabilities

IEC 62443-2-4:2015+AMD1:2017 CSV – 7 –
© IEC 2017

In Figure 2, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 3 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

NOTE 4 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

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.

“None”