

NEK 820:2021

Engelsk utgave 

# Cybersikkerhet for industrielle automatiserings- og kontrollsystemer

Generisk OT

Norsk elektroteknisk standardsamling



**NEK**

NORSK ELEKTROTEKNISK KOMITE



# Innholdsfortegnelse NEK 800:2021

## Cybersikkerhet for industrielle automatiserings- og kontrollsystemer

### Del 1:

NEK IEC TS 62443-1-1:2009 .....	1
---------------------------------	---

### Del 2:

NEK IEC 62443-2-1:2010 .....	92
NEK IEC TR 62443-2-3:2015 .....	261
NEK EN IEC 62443-2-4:2019.....	330
NEK EN IEC 62443-2-4:2019/A1:2019 .....	431

### Del 3:

NEK IEC TR 62443-3-1:2009 .....	460
NEK EN IEC 62443-3-2:2020 .....	571
NEK EN IEC 62443-3-3:2019 .....	709
NEK EN IEC 62443-3-3:2019/AC:2019-10	

### Del 4:

NEK EN IEC 62443-4-1:2018 .....	718
NEK EN IEC 62443-4-2:2019 .....	783



## Norsk forord

Cybersikkerhet er et aktuelt tema mer enn noen gang tidligere. Flere utredninger fra myndigheter og private aktører viser mot en sterk økning i cybertrusler mot samfunnskritisk infrastruktur. Dette kan være anlegg som kraftforsyning, transport, helse og samfunnskritiske forsyningstjenester.

Cybersikkerhet knyttes ofte opp mot informasjonsteknologi (IT) og operasjonell teknologi (OT). Denne standardsamlingen tar for seg hvordan man sikrer anlegg innen operasjonell teknologi (OT).

NEK 820 er en samling av hele NEK EN IEC 62443-serien og gir en strukturert tilnærming for å utlede sikkerhetskrav for industriell automatisering og kontrollsystemer (IACS).

NEK 820 er basert på følgende konsepter:

- **Fundamentale krav (FR):** NEK 820 definerer totalt syv grunnleggende krav med hensyn til sikkerheten til et industrielt automatisering og kontrollsystem (FR1, FR2, FR3, FR4, FR5, FR6 og FR7).
- **Sikkerhetsnivåer (SL):** NEK 820-standardene definerer sikring i form av fire forskjellige nivåer (SL1, SL2, SL3 og SL4), hver med et økende sikkerhetsnivå.

NEK 820 er ikke oversatt til norsk og foreligger i sin opprinnelige form på engelsk språk.

Standardene har over tid vært siktet inn mot industrielle anlegg, men de har også relevans og bred nytte for andre interessenter.

Standardserien er utviklet i et tett samarbeid mellom ISA99<sup>1)</sup> og IEC TC 65 WG 10<sup>2)</sup>, hvor det pågår revisjon av flere deler av serien. I tillegg arbeides det også med å bearbeide serien mot å bli en horisontal standard i IEC. Arbeidet speiles i Norge av normkomite NEK NK 65<sup>3)</sup> og arbeidsgruppe AG1 Cybersikkerhet.

Grunnet usikkerhet ved neste utgivelse av IEC 62443 vil det være vanskelig å sette stabilitetsdato for denne publikasjonen.

### **NEK 820 består av:**

#### **Del 1 – Generelt:**

NEK IEC TS 62443-1-1:2009

#### **Del 2 – Policy og prosedyrer**

NEK IEC 62443-2-1:2010

NEK IEC TR 62443-2-3:2015

NEK EN IEC 62443-2-4:2019

NEK EN IEC 62443-2-4:2019/A1:2019

### **Del 3 - System**

NEK IEC TR 62443-3-1:2009

NEK EN IEC 62443-3-2:2020

NEK EN IEC 62443-3-3:2019

NEK EN IEC 62443-3-3:2019/AC:2019-10

### **Del 4 - Komponent**

NEK EN IEC 62443-4-1:2018

NEK EN IEC 62443-4-2:2019

### **Kommentar fra komite NK65**

I NK65 ser vi at det er betydelig økt interesse for denne standardserien. Den brer godt om seg i bedriftene som er representert i komiteen, i flere andre bedrifter, samt innen industrien generelt i Norge og internasjonalt. Vi ser en god trend i retning av at standardserien vil kunne bli en horisontal standard.

Det gjøres oppmerksom på at noen delstandarder i serien er av eldre publiseringsdato. Det pågår betydelig arbeid for å harmonisere, styrke og fornye deler av standardserien. Fundamentene og prinsippene bak serien står seg likevel godt, og eldre delstandarder i denne serien er fortsatt godt anvendelige og hensiktsmessige å sette seg inn i.

Med graden av fornyingsarbeid som pågår vil vi oppfordre brukerne av serien til å lese og anvende den med en pragmatisk tilnærming, og gjerne søke etter kunnskap og informasjon om hvilken retning standarden beveger seg med hensyn til fundamentale prinsipper, krav og hvordan de ulike delstandardene er ment å utfylle hverandre.

### **Utgave 1 – versjon 1.0**

- 1) International society of Automation (ISA) – komite [ISA99](#).
- 2) International Electrotechnical Commission (IEC) – teknisk komite [IEC TC 65](#) – arbeidsgruppe WG 10.
- 3) Norsk Elektroteknisk Komite (NEK) – normkomite [NEK NK 65](#) arbeidsgruppe AG1 Cybersikkerhet.



# NEK IEC TS 62443-1-1:2009

*Engelsk versjon*

## Industrial communication networks

Network and system security

Part 1-1: Terminology, concepts and models

**Norwegian electrotechnical specification**









# IEC/TS 62443-1-1

Edition 1.0 2009-07

# TECHNICAL SPECIFICATION



---

**Industrial communication networks – Network and system security –  
Part 1-1: Terminology, concepts and models**



**THIS PUBLICATION IS COPYRIGHT PROTECTED****Copyright © 2009 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://www.iec.ch)

**About IEC publications**

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: [www.iec.ch/webstore/custserv](http://www.iec.ch/webstore/custserv)

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: [csc@iec.ch](mailto:csc@iec.ch)  
Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00



# IEC/TS 62443-1-1

Edition 1.0 2009-07

# TECHNICAL SPECIFICATION



---

**Industrial communication networks – Network and system security –  
Part 1-1: Terminology, concepts and models**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

PRICE CODE **XC**

---

ICS 25.040.40; 33.040.040; 35.040

ISBN 978-2-88910-710-0

## CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
1.1 General.....	8
1.2 Included functionality.....	8
1.3 Systems and interfaces.....	8
1.4 Activity-based criteria.....	9
1.5 Asset-based criteria.....	9
2 Normative references.....	10
3 Terms, definitions and abbreviations.....	10
3.1 General.....	10
3.2 Terms and definitions.....	10
3.3 Abbreviations.....	26
4 The situation.....	27
4.1 General.....	27
4.2 Current systems.....	27
4.3 Current trends.....	28
4.4 Potential impact.....	28
5 Concepts.....	29
5.1 General.....	29
5.2 Security objectives.....	29
5.3 Foundational requirements.....	30
5.4 Defence in depth.....	30
5.5 Security context.....	30
5.6 Threat-risk assessment.....	32
5.6.1 General.....	32
5.6.2 Assets.....	32
5.6.3 Vulnerabilities.....	34
5.6.4 Risk.....	34
5.6.5 Threats.....	36
5.6.6 Countermeasures.....	38
5.7 Security program maturity.....	39
5.7.1 Overview.....	39
5.7.2 Maturity phases.....	42
5.8 Policies.....	45
5.8.1 Overview.....	45
5.8.2 Enterprise level policy.....	46
5.8.3 Operational policies and procedures.....	47
5.8.4 Topics covered by policies and procedures.....	47
5.9 Security zones.....	50
5.9.1 General.....	50
5.9.2 Determining requirements.....	50
5.10 Conduits.....	51
5.10.1 General.....	51
5.10.2 Channels.....	52
5.11 Security levels.....	53

5.11.1	General .....	53
5.11.2	Types of security levels.....	53
5.11.3	Factors influencing SL(achieved) of a zone or conduit.....	55
5.11.4	Impact of countermeasures and inherent security properties of devices and systems.....	57
5.12	Security level lifecycle.....	57
5.12.1	General .....	57
5.12.2	Assess phase .....	58
5.12.3	Develop and implement phase .....	59
5.12.4	Maintain phase .....	60
6	Models .....	61
6.1	General .....	61
6.2	Reference models .....	62
6.2.1	Overview .....	62
6.2.2	Reference model levels.....	63
6.3	Asset models.....	65
6.3.1	Overview .....	65
6.3.2	Enterprise.....	68
6.3.3	Geographic sites.....	68
6.3.4	Area .....	68
6.3.5	Lines, units, cells, vehicles.....	68
6.3.6	Supervisory control equipment .....	68
6.3.7	Control equipment .....	68
6.3.8	Field I/O network .....	69
6.3.9	Sensors and actuators .....	69
6.3.10	Equipment under control.....	69
6.4	Reference architecture .....	69
6.5	Zone and conduit model.....	69
6.5.1	General .....	69
6.5.2	Defining security zones .....	70
6.5.3	Zone identification .....	70
6.5.4	Zone characteristics.....	74
6.5.5	Defining conduits .....	76
6.5.6	Conduit characteristics.....	77
6.6	Model relationships.....	79
	Bibliography.....	81
	Figure 1 – Comparison of objectives between IACS and general IT systems .....	29
	Figure 2 – Context element relationships.....	31
	Figure 3 – Context model .....	31
	Figure 4 – Integration of business and IACS cybersecurity.....	40
	Figure 5 – Cybersecurity level over time .....	40
	Figure 6 – Integration of resources to develop the CSMS.....	41
	Figure 7 – Conduit example.....	52
	Figure 8 – Security level lifecycle.....	58
	Figure 9 – Security level lifecycle – Assess phase .....	59
	Figure 10 – Security level lifecycle – Implement phase .....	60
	Figure 11 – Security level lifecycle – Maintain phase.....	61

Figure 12 – Reference model for IEC 62443 standards .....	62
Figure 13 – SCADA reference model .....	63
Figure 14 – Process manufacturing asset model example.....	66
Figure 15 – SCADA system asset model example.....	67
Figure 16 – Reference architecture example.....	69
Figure 17 – Multiplant zone example .....	71
Figure 18 – Separate zones example.....	72
Figure 19 – SCADA zone example.....	73
Figure 20 – SCADA separate zones example.....	74
Figure 21 – Enterprise conduit.....	77
Figure 22 – SCADA conduit example.....	78
Figure 23 – Model relationships.....	80
Table 1 – Types of loss by asset type .....	33
Table 2 – Security maturity phases .....	43
Table 3 – Concept phase .....	43
Table 4 – Functional analysis phase .....	43
Table 5 – Implementation phase.....	44
Table 6 – Operations phase .....	44
Table 7 – Recycle and disposal phase.....	45
Table 8 – Security levels .....	53

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –  
NETWORK AND SYSTEM SECURITY –****Part 1-1: Terminology, concepts and models**

## 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62443-1-1, which is a technical specification, has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This technical specification is derived from the corresponding US ANSI/S99.01.01 standard.



The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
65/423/DTS	65/432A/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

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

A list of all parts of the IEC 62433 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

NOTE The revision of this technical specification will be synchronized with the other parts of the IEC 62443 series.

**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 publication using a colour printer.**

## INTRODUCTION

The subject of this technical specification is security for industrial automation and control systems. In order to address a range of applications (i.e., industry types), each of the terms in this description have been interpreted very broadly.

The term “Industrial Automation and Control Systems” (IACS), includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

The term “security” is considered here to mean the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in IACS. Cybersecurity which is the particular focus of this technical specification, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

The audience for this technical specification includes all users of IACS (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, government organizations involved with, or affected by, control system cybersecurity, control system practitioners, and security practitioners. Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this technical specification is also a reference for those responsible for the integration of IACS and enterprise networks.

Typical questions addressed by this technical specification include:

- a) What is the general scope of application for IACS security?
- b) How can the needs and requirements of a security system be defined using consistent terminology?
- c) What are the basic concepts that form the foundation for further analysis of the activities, system attributes, and actions that are important to provide electronically secure control systems?
- d) How can the components of an IACS be grouped or classified for the purpose of defining and managing security?
- e) What are the different cybersecurity objectives for control system applications?
- f) How can these objectives be established and codified?

Each of these questions is addressed in detail in subsequent clauses of this technical specification.

# **INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –**

## **Part 1-1: Terminology, concepts and models**

### **1 Scope**

#### **1.1 General**

This part of the IEC 62443 series is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.

To fully articulate the systems and components the IEC 62443 series address, the range of coverage may be defined and understood from several perspectives, including the following:

- a) range of included functionality;
- b) specific systems and interfaces;
- c) criteria for selecting included activities;
- d) criteria for selecting included assets.

Each of these is described in the following subclauses:

#### **1.2 Included functionality**

The scope of this technical specification can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

This technical specification focuses primarily on industrial automation and control, as described in a reference model (see Clause 6). Business planning and logistics systems are not explicitly addressed within the scope of this technical specification, although the integrity of data exchanged between business and industrial systems is considered.

Industrial automation and control includes the supervisory control components typically found in process industries. It also includes SCADA (Supervisory Control and Data Acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include the following:

- a) electricity transmission and distribution;
- b) gas and water distribution networks;
- c) oil and gas production operations;
- d) gas and liquid transmission pipelines.

This is not an exclusive list. SCADA systems may also be found in other critical and non-critical infrastructure industries.

#### **1.3 Systems and interfaces**

In encompassing all IACS, this technical specification covers systems that can affect or influence the safe, secure, and reliable operation of industrial processes. They include, but are not limited to:

- a) Industrial control systems and their associated communications networks<sup>1</sup>, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. (In this context, industrial control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.)
- b) Associated systems at level 3 or below of the reference model described in Clause 6. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, pipeline leak detection systems, work management, outage management, and electricity energy management systems.
- c) Associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

#### 1.4 Activity-based criteria

IEC 62443-2-1<sup>2</sup> provides criteria for defining activities associated with manufacturing operations. A similar list has been developed for determining the scope of this technical specification. A system should be considered to be within the range of coverage of the IEC 62443 series if the activity it performs is necessary for any of the following:

- a) predictable operation of the process;
- b) process or personnel safety;
- c) process reliability or availability;
- d) process efficiency;
- e) process operability;
- f) product quality;
- g) environmental protection;
- h) regulatory compliance;
- i) product sales or custody transfer.

#### 1.5 Asset-based criteria

The coverage of this technical specification includes those systems in assets that meet any of the following criteria, or whose security is essential to the protection of other assets that meet these criteria:

- a) The asset has economic value to a manufacturing or operating process.
- b) The asset performs a function necessary to operation of a manufacturing or operating process.
- c) The asset represents intellectual property of a manufacturing or operating process.
- d) The asset is necessary to operate and maintain security for a manufacturing or operating process.
- e) The asset is necessary to protect personnel, contractors, and visitors involved in a manufacturing or operating process.
- f) The asset is necessary to protect the environment.

---

<sup>1</sup> The term “communications networks” includes all types of communications media, including various types of wireless communications. A detailed description of the use of wireless communications in industrial automation systems is beyond the scope of this technical specification. Wireless communication techniques are specifically mentioned only in situations where their use or application may change the nature of the security applied or required.

<sup>2</sup> To be published.

- g) The asset is necessary to protect the public from events caused by a manufacturing or operating process.
- h) The asset is a legal requirement, especially for security purposes of a manufacturing or operating process.
- i) The asset is needed for disaster recovery.
- j) The asset is needed for logging security events.

This range of coverage includes systems whose compromise could result in the endangerment of public or employees health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, environmental contamination, and/or economic loss or impact on an entity or on local or national security.

## 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.

IEC 62264-1, *Enterprise-control system integration – Part 1: Models and terminology*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

## 3 Terms, definitions and abbreviations

### 3.1 General

Wherever possible, definitions have been adapted from those used in established industry sources. Some definitions have been adapted from more generic definitions used in the IT industry.

### 3.2 Terms and definitions

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

#### 3.2.1

##### **access**

ability and means to communicate with or otherwise interact with a system in order to use system resources

NOTE Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log in to a system and application, through a combination of logical and physical means).

#### 3.2.2

##### **access control**

protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy [10]<sup>3</sup>

[RFC 2828, modified]

---

<sup>3</sup> Numbers in square brackets refer to the Bibliography.