

NEK 850A:2025

Cybersikkerhet for protokoller og informasjonsutveksling i elkraftsystemet *Energi OT*

Norsk elektroteknisk standardsamling

Engelsk utgave 



NEK 850 A:2025

**Cybersikkerhet for protokoller og
informasjonsutveksling i elkraftsystemet Energi
OT**

Norsk elektroteknisk standardsamling



INNHold

Nasjonalt Forord	4
Innledning	5
NEK IEC TS 62351-1:2007	7
NEK IEC TS 62351-2:2008	42
NEK IEC 62351-3:2023	105
NEK IEC 62351-4:2018	157
NEK IEC 62351-4:2018/AMD1:2020	319
NEK IEC 62351-5:2023	362
NEK IEC 62351-6:2020	473
NEK IEC 62351-7:2017	512
NEK IEC 62351-8:2020	713
NEK IEC 62351-9:2023	789
NEK IEC TR 62351-10:2012	939
NEK IEC 62351-11:2016	990

Nasjonalt Forord

- 1) Norsk Elektroteknisk Komite (NEK) er det norske medlemmet i IEC (International Electrotechnical Commission) og CENELEC (European Committee for Electrotechnical Standardization). NEKs formål er å fremme internasjonalt, europeisk og nasjonalt samarbeid knyttet til standardisering. NEK publiserer standarder og andre teknisk relaterte dokumenter utviklet av NEK, IEC og/eller Cenelec, heretter kalt NEK-publikasjoner. Enhver person med interesse og kompetanse kan delta i utvikling av NEK-publikasjoner. Myndigheter, industri og ikke-offentlige organisasjoner kan delta.
- 2) De formelle beslutningene i NEK som gjelder tekniske saker er basert på, så langt det er praktisk mulig, konsensus mellom interessentene organisert gjennom NEKs tekniske komiteer.
- 3) Denne publikasjonen har krav, anbefalinger og/eller informasjon for nasjonal bruk. Selv om det gjøres mye for å sikre at innholdet i NEK-publikasjoner er korrekt, kan NEK ikke holdes ansvarlig for måten de benyttes på, eventuelle feil, eller feiltolkninger gjort av brukeren.
- 4) For å bidra til internasjonal harmonisering brukes EN IEC-publikasjoner når dette er mulig. Eventuelle forskjeller mellom EN IEC-publikasjoner og NEK-publikasjoner som NEK er gjort kjent med, synliggjøres for brukeren.
- 5) NEK utfører ikke samsvarsvurderinger. Selvstendige sertifiseringsorganisasjoner utfører slike tjenester. NEK er ikke ansvarlig for tjenester utført av tredjepart, eksempelvis et sertifiseringsselskap.
- 6) Alle brukere bør forsikre seg om at de har anskaffet den korrekte versjonen av denne publikasjonen.
- 7) NEK eller dets ledere, ansatte, innleide, hjelpere, individuelle eksperter og medlemmer av standardiseringsgrupper, er ikke ansvarlig for personskade, materiellskade eller annen skade av noe slag, direkte eller indirekte, eller for kostnader (inkludert saksomkostninger) og utlegg relatert til, bruk av, eller referanse til, denne NEK-publikasjonen eller andre NEK-publikasjoner.
- 8) Merk at eventuelle normative referanser referert i denne publikasjonen er nødvendige for riktig forståelse av denne publikasjonen.
- 9) Merk muligheten for at elementer i denne NEK-publikasjonen kan være gjenstand for patentrettigheter. NEK skal ikke holdes ansvarlig for å identifisere patentrettigheter.

NEK 850 A samlingen er utarbeidet av NEKs administrasjon. Dokumentet er en samling av IEC Standarder utviklet i teknisk komite IEC TC 57 Power systems management and associated information exchange, der norske bidrag er gitt via den norske speilkomiteen NK 57 -Informasjonsforvaltning for elkraftsystemet. Det vises til denne samlingen i NVE sin veileder til kraftberedskapsforskriften (KBF).

Dette dokumentet er gyldig fra publikasjonsdato og fastsetter ingen overgangstid for gyldigheten av tidligere utgaver.

Eventuelle tolkninger og rettelser til dette dokumentet kan bli publisert på www.nek.no. De finnes også på nettbutikken vår. www.standard.no

Innledning

Digitaliseringen i elkraftsystemet øker, og med dette kravene til cybersikkerhet. Driftssentral- og kontrollsystemer har høye krav til sikring, og innenfor denne operative teknologien (OT) er det kritisk viktig at relevante risikoreduserende tiltak iverksettes når det er aktuelt. Denne samlingen inneholder beskrivelser og krav til hvordan mange av tiltakene etter internasjonalt anerkjente metoder kan implementeres. Herunder kryptering av samband og informasjonsutveksling, samt rollebasert aksesskontroll.

Standardserien NEK IEC 62351 Data and communications security inneholder standarder og tekniske spesifikasjoner som benyttes for sikring av kritisk infrastruktur i elkraftsystemet. I denne del A finnes de mest brukte standardene for krav til sikring av protokoller og informasjonsutveksling, mens del B inneholder standarder for veiledning i bruk og standarder for krav til prøving av systemer som har implementert de tekniske kravene i del A.

Samlingen inneholder flere steder også henvisninger til IEC 62443, en serie som er utgitt i den norske NEK-samlingen NEK 820.

Kravene i dette dokumentet er gjennomgående formulert på en bestemt måte med tanke på å øke forståelsen av hva de forskjellige kravene innebærer og hvilken tyngde bestemte ord har. «ISO/IEC Directives 2» beskriver dette nærmere, men deler av dette er gjengitt som følger:

- Skal (shall): Kravtekst formulert med «skal» er et krav som ikke kan fravikes. Det kan forekomme betingelser knyttet til kravet, men om disse betingelsene er til stede, er det ikke mulighet for fravik.
- Bør (should): Kravtekst formulert med «bør» innebærer en sterk anbefaling. Den kan fravikes, men underforstått skal det sterke faglige grunner til for ikke å følge anbefalingen. Formuleringen «bør» leses som et krav om etterlevelse, men ikke nødvendigvis for alle situasjoner.
- Kan (may): Kravtekst formulert med «kan» innebærer en mulighet, eller en akseptert løsning.

NASJONAL MERKNAD ISO/IEC regelverket skiller på «may» og «can». På norsk er dette problematisk, noe som i visse tilfeller fører til omskriving eller bruk av hjelpeverbet «kan», både for «may» og for «can». Forskjellen på «may» og «can» i norsk oversettelse fremkommer av kontekst. «Can» brukes rent informativt og er ikke en akseptformulering.

TECHNICAL SPECIFICATION

**Power systems management and associated information exchange –
Data and communications security – Part 1: Communication network and system
security – Introduction to security issues**



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2007 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.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

TECHNICAL SPECIFICATION

**Power systems management and associated information exchange –
Data and communications security – Part 1: Communication network and system
security – Introduction to security issues**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 2831891388

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

CONTENTS

NEK IEC TS 62351-1:2007	6
FOREWORD	7
1 Scope and object	9
1.1 Scope	9
1.2 Object	9
2 Normative references	10
3 Terms, definitions and abbreviations	10
4 Background for information security standards	10
4.1 Rationale for addressing information security in power system operations	10
4.2 IEC TC 57 data communications protocols	11
4.3 History of the Development of these Security Standards	11
5 Security issues for the IEC 62351 series	12
5.1 General information on security	12
5.2 Types of security threats	12
5.2.1 General	12
5.2.2 Inadvertent threats	13
5.2.3 Deliberate threats	14
5.3 Security requirements, threats, vulnerabilities, attacks, and countermeasures	15
5.3.1 Security requirements	15
5.3.2 Security threats	15
5.3.3 Security vulnerabilities	16
5.3.4 Security attacks	16
5.3.5 Security Categories	16
5.3.6 Security Countermeasures	17
5.3.7 Decomposing the security problem space	19
5.4 Importance of security policies	19
5.5 Security risk assessment	20
5.6 Understanding the security requirements and impact of security measures on power system operations	20
5.6.1 Security challenges in power system operations	20
5.6.2 Key management and certificate revocation	21
5.6.3 System and network management	21
5.7 Five-step security process	22
5.8 Applying security to power system operations	23
6 Overview of the IEC 62351 series	24
6.1 Scope of the IEC 62351 series	24
6.2 Authentication as key security requirement	24
6.3 Objectives of the IEC 62351 series	24
6.4 Relationships between the IEC 62351 parts and IEC protocols	25
6.5 IEC 62351.1: Introduction	26
6.6 IEC 62351.2: Glossary of terms	26
6.7 IEC 62351.3: Profiles including TCP/IP	26
6.7.1 Threats and types of attacks being countered	26
6.7.2 Security requirements and measures	27
6.7.3 Usage of VPN tunnels and bump-in-the-wire technology	28
6.8 IEC 62351.4: Security for profiles that include MMS	28

6.8.1 Threats and types of attacks being countered	28
6.8.2 Security requirements and measures	28
6.9 IEC 62351.5: Security for IEC 60870.5 and derivatives	29
6.9.1 Threats and types of attacks being countered	29
6.9.2 Security requirements and measures	29
6.9.3 Possible additional security measures to IEC 62351.5	29
6.10 IEC 62351.6: Security for IEC 61850 Profiles	29
6.10.1 Threats and types of attacks being countered	29
6.10.2 Security requirements and measures	30
6.11 IEC 62351.7: Security through network and system management	31
6.11.1 Purpose and scope of IEC 62351.7	31
6.11.2 NSM Requirements	32
6.11.3 Examples of NSM data objects	32
7 Conclusions	34
Bibliography	35

Figure 1 – Security requirements, threats, and possible attacks	16
Figure 2 – Security categories, typical attacks, and common countermeasures	16
Figure 3 – Confidentiality security countermeasures	17
Figure 4 – Integrity security countermeasures	17
Figure 5 – Availability security countermeasures	18
Figure 6 – Non-repudiation security countermeasures	18
Figure 7 – Overall security: security requirements, threats, countermeasures, and management	18
Figure 8 – General security process – continuous cycle	22
Figure 9 – Correlation between the IEC 62351 series and IEC TC 57 profile standards	26
Figure 10 – Authentication security measure in GOOSE/SMV	31
Figure 11 – NSM object models are the information infrastructure equivalent to the CIM and IEC 61850 object models of the power system infrastructure	32
Figure 12 – Power system operations systems, illustrating the security monitoring architecture	32

Table 1 – Characteristics of the three multicast IEC 61850 protocols	30
Table 2 – Security measures for the three multicast IEC 61850 protocols	30

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION
EXCHANGE –**

**Data and communications security –
Part 1: Communication network and system security –**

Introduction to security issues

NEK IEC TS 62351-1:2007

Power systems management and associated information exchange - Data and communications security
- Part 1: Communication network and system security - Introduction to security issues