Norsk
Elektroteknisk
Komite

NEK 850B:2025

Cybersikkerhet for protokoller og informasjonsutveksling i elkraftsystemet

Energi OT - Tekniske spesifikasjoner og rapporter

Norsk elektroteknisk publikasjonssamling

Engelsk utgave

NEK 850B:2025

Cybersikkerhet for protokoller og informasjonsutveksling i elkraftsystemet

Energi OT - Tekniske spesifikasjoner og rapporter

Norsk elektroteknisk publikasjonssamling

© NEK har opphavsretten til denne publikasjon.
Ingen del av materialet må reproduseres på noen form for medium uten skriftlig avtale med NEK.

INNHOLD

Nasjonalt Forord 4

Innledning 5

NEK IEC TR 62351-12:2016 6

NEK IEC TR 62351-13:2016 115

NEK IEC TR 62351-90-1:2018 153

NEK IEC TR 62351-90-2:2018 240

NEK IEC TR 62351-90-3:2021 272

NEK IEC TS 62351-100-1:2018 300

NEK IEC TS 62351-100-3:2020 397

NEK IEC TS 62351-100-4:2023 428

NEK IEC TS 62351-100-6:2022 542

 © NEK 2025

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 B samlingen er utarbeidet av NEKs adminsitrasjon. 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 B finnes standarder for veiledning i bruk og standarder for krav til prøving av systemer som har implementert de tekniske kravene i del A, mens del A inneholder de mest brukte standardene for krav til sikring av protokoller og informasjonsutveksling.

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.

 © NEK 2025

NEK IEC TR 62351-12

Edition 1.0 2016-04

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

NEK IEC TR 62351-12:2016 ED1

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2016 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 Varembé
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.

NEK IEC TR 62351-12

Edition 1.0 2016-04

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

INTERNATIONAL
ELECTROTECHNCIAL
COMMISSION

ICS 33.200

ISBN 9782832232552

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

NEK IEC TR 62351-12:2016 7
FOREWORD 8
INTRODUCTION 10
1 Scope 12
2 Normative references 12
3 Terms and definitions 13
4 Abbreviations and acronyms 14
5 architectures and cyber-physical concepts 15
5.1 Resiliency challenge for power systems with systems 15
5.2 Five-level hierarchical architecture 16
5.3 system interfaces 18
5.4 Resilience at different architectural levels 19
5.5 Systems as cyber-physical systems 20
5.5.1 Protecting cyber-physical systems 20
5.5.2 Cyber-physical threats 21
5.5.3 Resilience measures for cyber-physical systems 22
6 Threats, vulnerabilities, and impacts on power system resilience 24
6.1 Threats – engineering and cyber 24
6.1.1 Physical and electrical threats – mostly but not entirely inadvertent 24
6.1.2 Cyber threats – inadvertent and deliberate 24
6.2 Vulnerabilities – engineering and cyber vulnerabilities 27
6.2.1 General 27
6.2.2 Power system vulnerabilities and attacks 28
6.2.3 Cyber security vulnerabilities and attacks 30
6.3 Risk management and mitigation techniques 31
6.3.1 Risk handling 31
6.3.2 Risk mitigation categories 32
6.4 Impacts on power system resilience 34
6.4.1 Safety impacts 34
6.4.2 Power outage impacts 35
6.4.3 Power quality impacts 35
6.4.4 Financial impacts 36
6.4.5 Regulatory and legal impacts 36
6.4.6 Environmental impacts 37
6.4.7 Goodwill and other “soft” impacts 37
6.5 stakeholders' resilience responsibilities 37
6.6 Resilience Measures for systems to counter threats 38
6.6.1 General IT cyber security approach for systems 38
6.6.2 Resilience by engineering designs and operational strategies 39
7 Level 1 System resilience recommendations 39
7.1 General 39
7.2 Level 1 system: architecture 39
7.3 Level 1 system: vulnerabilities 40
7.3.1 General 40
7.3.2 Cyber vulnerabilities 40
7.3.3 Engineering design and development vulnerabilities 41

7.3.4 Deployment and operational vulnerabilities ... 42
7.4 Level 1 system: impacts ... 42
7.5 Level 1 system: resilience recommendations ... 44
7.5.1 General ... 44
7.5.2 Manufacturer: system design for resilience recommendations ... 45
7.5.3 Integrator and installer: setup for meeting resilience recommendations ... 47
7.5.4 Testing personnel: resilient system interconnection testing recommendations ... 48
7.5.5 user: access recommendations ... 49
7.5.6 designers: requirements for local communications ... 50
7.5.7 Security managers: alarming, logging, and reporting cyber security recommendations ... 51
7.5.8 Maintenance personnel: resilience recommendations for maintenance, updating and re-testing, systems ... 52
7.5.9 Recommended coping actions during an attack or failure ... 53
7.5.10 Recommended recovery and analysis actions after an attack or failure ... 54
8 Level 2: Facilities energy management () resilience recommendations ... 55
8.1 Level 2 : architecture ... 55
8.2 Level 2 : Vulnerabilities ... 56
8.3 Level 2 : Impacts ... 57
8.4 Level 2 : Resilience recommendations ... 59
8.4.1 General ... 59
8.4.2 Manufacturer: Design of resilience recommendations ... 59
8.4.3 Integrators and installer: implementation for meeting resilience recommendations ... 60
8.4.4 Testing personnel: Resilient testing recommendations ... 62
8.4.5 users: Access recommendations ... 63
8.4.6 designers: Resilience recommendations ... 64
8.4.7 Security managers: Alarming, logging, and reporting recommendations ... 65
8.4.8 Maintenance personnel: Resilience recommendations for maintenance, updating and re-testing, systems ... 66
8.4.9 Recommended coping actions during an attack or failure ... 67
8.4.10 Recommended recovery and analysis actions after an attack or failure ... 68
9 Level 3: Third parties: Retail energy provider or aggregators resilience recommendations ... 68
9.1 Level 3: Third parties: architecture ... 68
9.2 Level 3: Third parties: vulnerabilities ... 69
9.3 Level 3: Third parties: impacts ... 70
9.4 Level 3: Third parties : Resilience recommendations ... 71
9.4.1 Third party designers: Resilience recommendations ... 71
9.4.2 users: Access recommendations ... 72
10 Level 4: Distribution operations analysis resilience recommendations ... 73
10.1 Level 4 analysis: Architecture ... 73
10.2 Level 4 analysis: Vulnerabilities ... 74
10.3 Level 4 analysis: Impacts ... 75
10.4 Level 4 analysis: Resilience recommendations ... 77
10.4.1 Resilient design of distribution grid equipment with systems ... 77
10.4.2 Resilience through grid operations with systems ... 77
10.4.3 Resilience through power system analysis ... 78
10.4.4 Resilience by stakeholder training ... 79
Annex A NISTIR 7628 Smart Grid Catalog of Security Requirements ... 80
A.1 NISTIR 7628 families of security requirements ... 80

A.2 Detailed NISTIR 7626 Catalogue of Smart Grid Security Requirements 81
Annex B IT security guidelines 86
B.1 Overview of cyber security issues for systems 86
B.2 Security guidelines and policies across organizational boundaries 86
B.3 User and device authentication 89
B.4 Good practices for specifying and implementing cryptography 92
B.5 Cryptographic methods 92
B.6 Cryptography used for transport layer security on networks 93
B.7 Wireless cryptography 94
B.8 Key management using Public Key Cryptography 94
B.9 Multicast and group keys 95
B.10 Device and platform integrity 96
B.11 Resilient network configurations 96
B.12 Network and system management () 96
B.13 Some additional cyber security techniques 96
B.14 Security testing procedures 97
B.15 Security interoperability 97
Annex C Mapping between IEC 62443_3_3, NISTIR 7628, and IEC TR 62351_12 99
C.1 Mapping table 99
C.2 IEC TR 62351_12 cyber security items not mapped to all guidelines 105
Annex D Glossary of terms 107
Bibliography 108

Figure 1 – Smart grid resilience: intertwined IT cyber security and engineering strategies 11
Figure 2 – Smart Grid Architecture Model (SGAM) 17
Figure 3 – Five-level hierarchical system architecture 17
Figure 4 – Structure of use cases within the hierarchy 20
Figure 5 – Mitigations by engineering strategies and cyber security measures 22
Figure 6 – Security requirements, threats, and possible attacks 31
Figure 7 – Level 1: Autonomous systems at smaller customer and utility sites 40
Figure 8 – Level 2 architecture 55
Figure 9 – third parties: Retail energy provider or aggregators architecture 69
Figure 10 – Distribution operations architecture 74

Table 1 – Examples of mitigations by engineering strategies and cyber security techniques 23
Table 2 – Engineering and cyber security data for managing the resilience of systems 23
Table 3 – Examples of mitigation categories for cyber-physical systems 33
Table 4 – Level 1 impact severities due to attacks and failures of autonomous systems 44
Table 5 – Level 2 impact severities due to malicious attacks and failures of 58
Table 6 – Level 3 impact severities due to malicious attacks and failures of 71
Table 7 – Level 4 impact severities due to malicious attacks and failures of or 76
Table A.1 – NIST Smart Grid Security Requirements Families 80
Table A.2 – Detailed NIST Catalogue of Smart Grid Security Requirements 81
Table C.1 – Mapping between IEC 62443_3_3, NISTIR 7628, and IEC TR 62351_12 100
Table C.2 – IEC 62351_12 cyber security items not mapped to all guidelines 106

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE –

Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

NEK IEC TR 62351-12:2016

Power systems management and associated information exchange - Data and communications security - Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems