Белорусский государственный университет транспорта
Гомель, Республика Беларусь

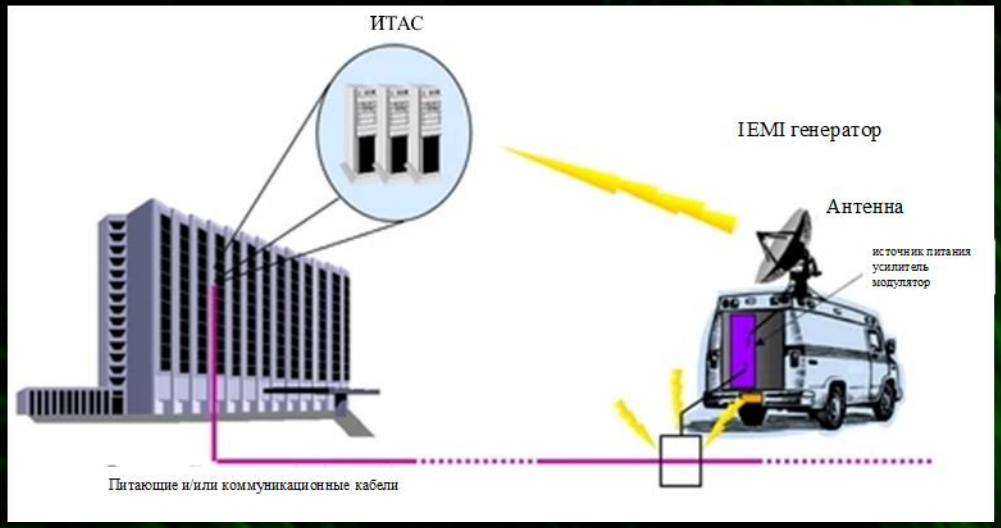
АНАЛИЗ И ПРОГНОЗИРОВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ К ЭЛЕКТРОМАГНИТНЫМ ИМПУЛЬСАМ ПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ

БОЧКОВ К.А. д.т.н., профессор
КОМНАТНЫЙ Д.В. к.т.н., доцент
ЖИГАЛИН И.О. м.т.н.

Научно-исследовательская лаборатория
«БЕЗОПАСНОСТЬ И ЭМС ТЕХНИЧЕСКИХ СРЕДСТВ»

Электромагнитный терроризм (ЭМТ) – воздействие преднамеренной электромагнитной помехой (ПЭМП, Intentional Electromagnetic Interference (IEMI)) на микроэлектронную элементную базу.

Под преднамеренной электромагнитной помехой, понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование.



Воздействие ПЭМП на микроэлектронные системы возможно, как по цепям питания, интерфейсным линиям, так и через свободное пространство.

SECRET – **SEC**urity of the **R**ailways against **E**lectromagnetic a**T**tacks (Защита железнодорожных систем от воздействия электромагнитных атак)

SECRET
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

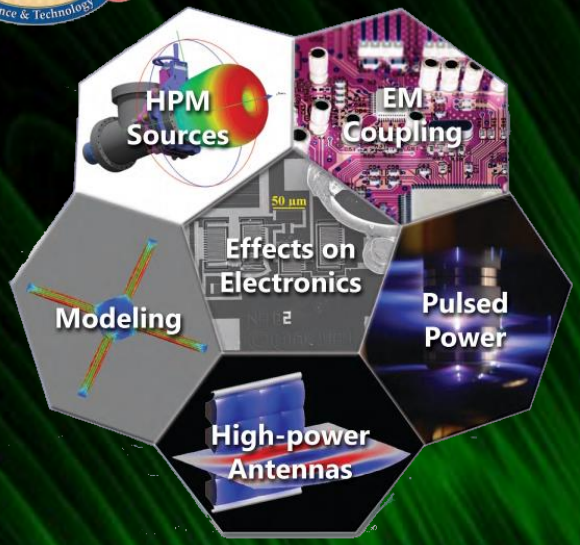
Цель проекта: анализ влияния ЭМ атак на европейскую железнодорожную сеть.
Задачи:

1. Оценка угроз и анализ рисков ЭМ атак
2. Техническая защита АПК СЖАТ и беспроводной связи (функциональная и информационная безопасность)
3. Разработка рекомендаций по повышению устойчивости ж.д. инфраструктуры от ЭМ атак (включая организационные и технические мероприятия)

Исследования в области микроволновых излучений (по данным открытых источников)

Protection of Critical Infrastructures against High Power Microwave Threats (HIPOW)

(Защита критически важной инфраструктуры от угроз со стороны микроволнового излучения высокой мощности)



Office of Naval Research (ONR)

(Управление военно-морских исследований)

Directed Energy Weapons (DEW)

(Направленное энергетическое оружие)

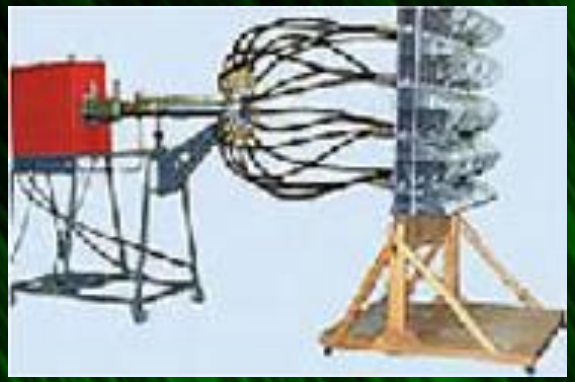
High Power Microwave (HPM) Program

(Программа фундаментальных исследований микроволн)

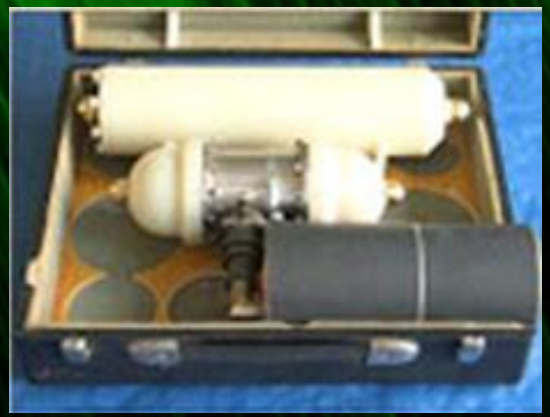
(Имеется лишь общая информация годового отчета за за 2021г.)

Генераторы направленного электромагнитного излучения

Техническими средствами создания ЭИПВ, как правило, являются специальные генераторы с узконаправленными антеннами сверхкоротких электромагнитных импульсов, как большие стационарные, так и малогабаритные переносные.



Сверхмощные ультраширокополосные импульсные генераторы



Носимые генераторы

Особенности электромагнитного терроризма

Для понимания механизмов проникновения ЭИПВ и принятия необходимых организационных и технических решений, предотвращения или уменьшения рисков деструктивного воздействия на критическую инфраструктуру необходимо учитывать следующее:

Угроза электромагнитного терроризма возрастает при применении малогабаритных генераторов ЭИПВ в связи с развитием мощной твердотельной электроники (сверхбыстродействующих полупроводниковых коммутаторов) с одной стороны и использование накопителей (современных) энергии с другой стороны

Электромагнитный терроризм с использованием ЭИПВ может осуществляться тайно и анонимно без особого ослабления через стены, стеклянные ограждения и т.д.

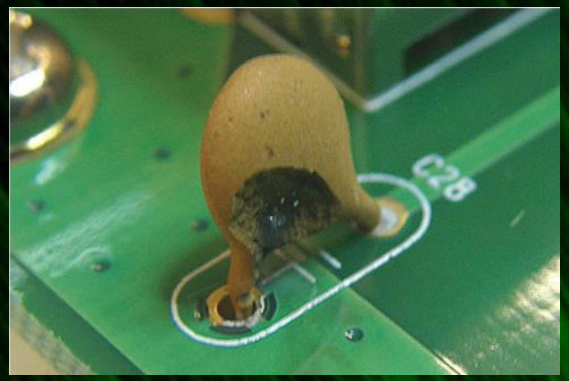
Направлен на нарушение требований по ФБ и ИБ КСИИ КВОИ ответственных технологических процессов (безопасности движения поездов).

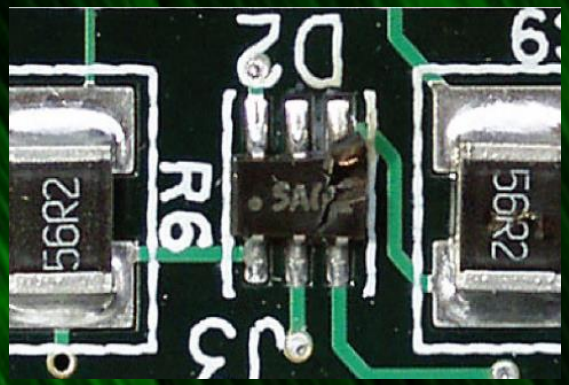
Необходимы дополнительные исследования механизмов проникновения ЭИПВ и методов защиты.

Повреждения от преднамеренного электромагнитного воздействия

Наибольшую опасность для критической инфраструктуры ИТ и АСУ ТП представляют малогабаритные переносные наносекундные импульсные генераторы, излучающие энергию в диапазоне до 10 ГГц. Воздействие таким генератором с близкого расстояния может вывести из строя до 20 компьютеров.

Это связано как с высоким быстродействием современных микроэлектронных компонентов, так и с низким значением напряжения пробоя переходов. Так, например, у запоминающих устройств пороговое напряжение составляет порядка 7 В, а логических интегральных микросхем на МОП-структурах от 7 до 15 В.





Современные компьютеры в небезопасном исполнении

Использование современных компьютеров (модных у молодежи) в критической инфраструктуре ИТ опасно из-за высокой проницаемости энергии ЭИПВ через неоднородности экранов, наличия радиопрозрачных стенок и вентиляционных отверстий.

Последствия нарушения работы АПК критической инфраструктуры и АСУ ТП в различных сферах применения

Сферы применения	Возможные последствия
Управление ответственными технологическими процессами	Инициирование запроектных аварий для вывода из строя технологического оборудования, остановка/ замедление технологических процессов.
Мониторинг и кризисное управление	Выход кризисной ситуации из под контроля, неадекватное управление ситуацией с непредсказуемыми последствиями.
Энергетика	Нарушение электроснабжения предприятий, инициирование аварий систем электроснабжения.
Транспорт	Нарушение работы систем обеспечения безопасности движения поездов; нарушение управления транспортными перевозками и контроля над ними.

Последствия успешной кибератаки

Широко известный случай используя уязвимости операционных систем и особенностей АСУ ТП на основе SCADA Siemens SIMATIC вирус Stuxnet вывел из строя 1368 из 5000 центрифуг на обогатительном предприятии.

Издание New York Times считает, что эта программа была разработана совместно разведывательными службами США и Израиля в 2009г. Бывший госсекретарь США Хиллари Клинтон в 2011 году заявила, что проект по разработке вируса Stuxnet оказался успешным и иранская ядерная компания будет отброшена на несколько лет назад.

Согласно исследованиям команды SCADA StrangeLove, представленным на Chaos Communication Congress в Германии, большая часть уязвимостей выявлена в продуктах крупных производителей: Siemens, Honeywell, Schneider Electric, причем соотношение устраненных и выявленных уязвимостей составляет около 65%, т.е. около 35% известных уязвимостей не имеют решения.

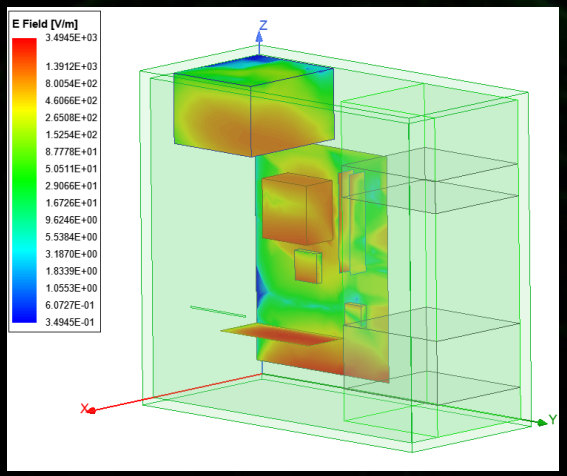
Учитывая это и выполненный в ЕС проект SECRET в ОАО РЖД очень своевременно была принята программа импортозамещения на 2017-2023 гг.

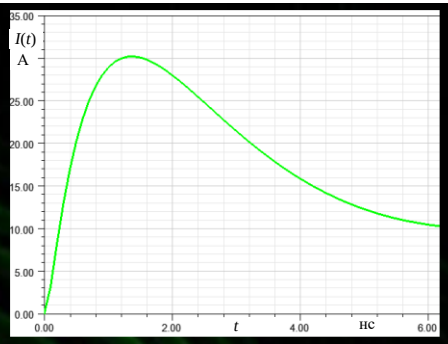
Методы анализа воздействия ЭИПВ на микропроцессорные технически средства

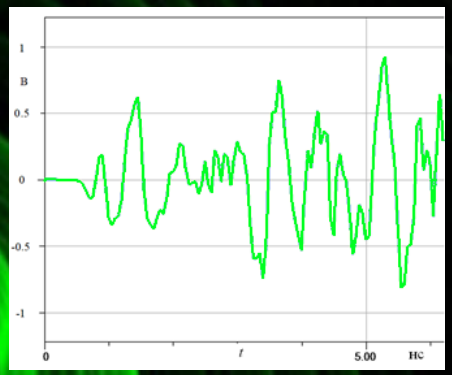
Методы анализа	Недостатки
Физическое моделирование	1. Дорогое, малодоступное, зачастую уникальное оборудование генераторов ЭИПВ 2. Разрушающий характер испытаний 3. Для выявления механизма проникновения и повреждения аппаратуры требуется программа длительных экспериментов
Математическое моделирование численными методами конечных элементов	1. Присущие численным методам внутренние ограничения сходимости и устойчивости 2. Методы реализованы в программах третьих производителей, которые не декларируют ограничения заложенных ими методов 3. Существенные затраты времени на разработку адекватной модели

Пример моделирования численным методом конечных элементов (Ansys ED)

(импульс по ГОСТ 30804.4.2, IEC 61000-4-2: $t_ф$= 0,8 нс, $t_и$= 5 нс)





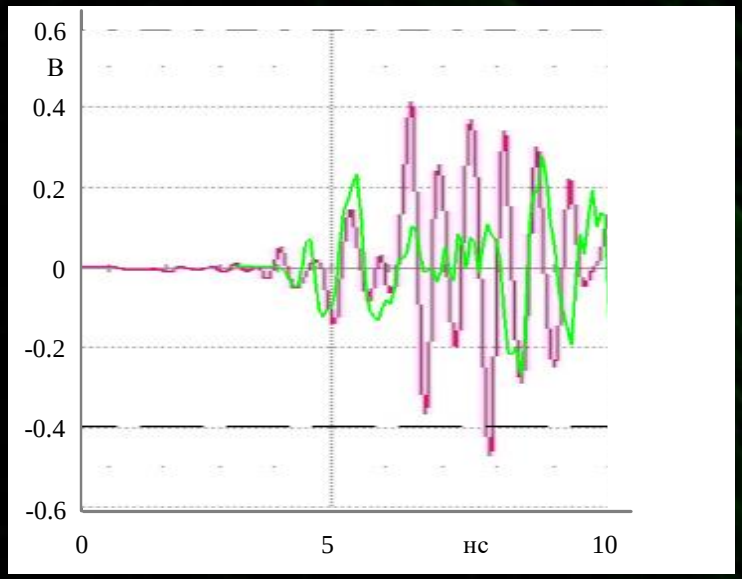


Из-за большого объёма вычислений методы моделирования не позволяют в полной мере решать задачи прогнозирования воздействия ЭИПВ, т.к. построение математической модели и расчёт характеристик для электродинамических систем сложной конфигурации часто является слишком трудоёмкой задачей.

Методу конечных элементов присущи погрешности, связанные с:

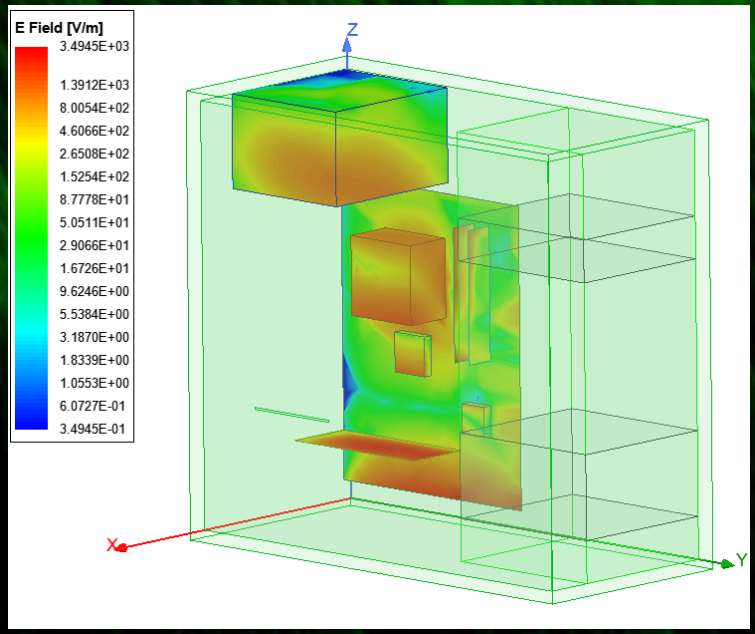
- ошибками дискретизации (результат геометрических различий границы рассматриваемой области и ее модели);
- ошибками базисной функции (обусловленными разностью между точным решением и его представлением);
- ошибками округления (связанными с конечной длиной разрядной сетки компьютера).

Сравнение результатов испытаний и моделирования



Результат моделирования

Результат измерения



Анализ и прогнозирование устойчивости критической инфраструктуры к воздействию ЭИПВ

Суть предлагаемого нами метода анализа и прогнозирования устойчивости критической инфраструктуры к воздействию ЭИПВ заключается в следующем:

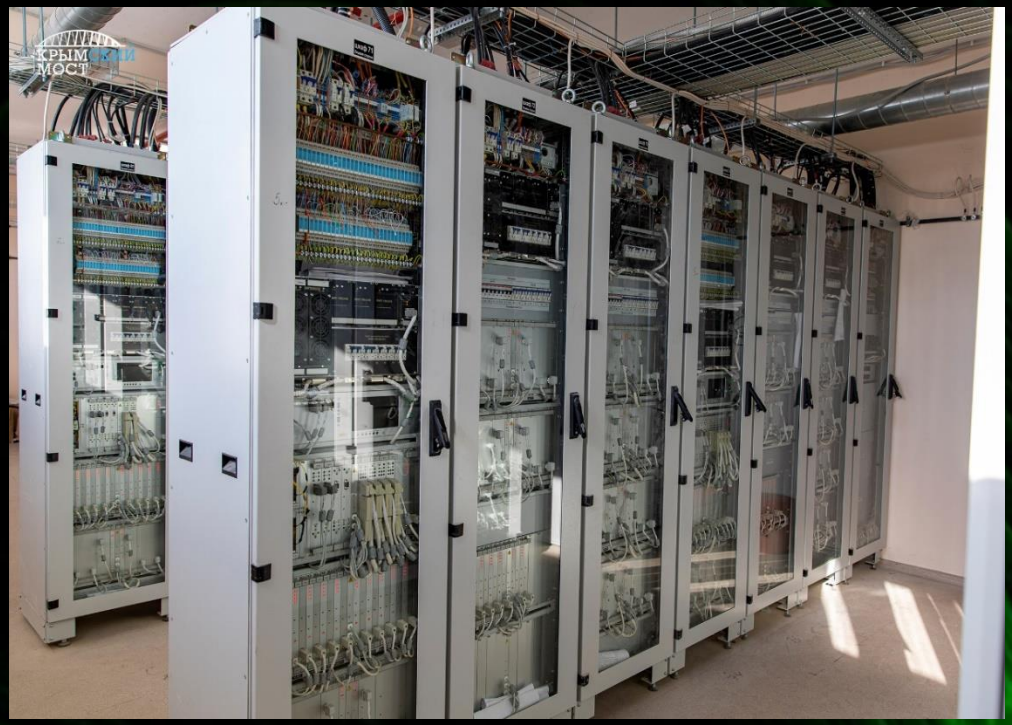
1) Стандартными генераторами ЭСР по ГОСТ 30804.4.2-2013 и ГОСТ Р 56115-2014 проводятся испытательные воздействия на неоднородности корпусов аппаратных средств критической инфраструктуры контактным ЭСР с возрастающей амплитудой испытательных импульсов до появления устойчивых сбоев (или отказов).

2) Полученное значение амплитуды импульса ЭСР является основой для решения двух взаимосвязанных задач:

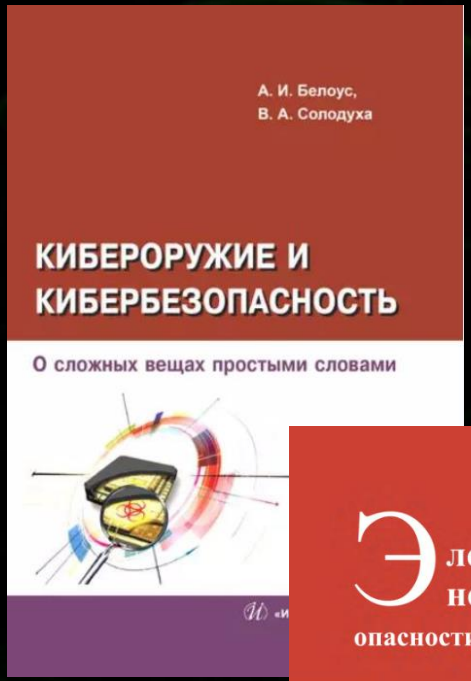
- **Определение размеров периметров охраны** объектов КИ на основе разработанных в НИЛ «БЭМС ТС» аналитических моделей проникновения ЭИПВ через неоднородности экранов и процессов затухания энергии от генераторов ЭИПВ

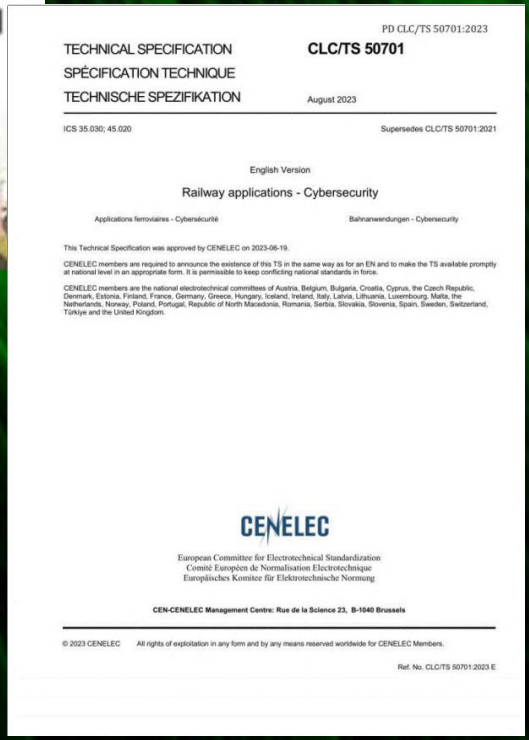
- **Определяется мощность генератора ЭИПВ** (в КУ антенны), воздействие которого с определенного расстояния способно вызвать сбой или отказ КИ.

Микроэлектронные АПК МПЦ станций и переездной сигнализации с радиопрозрачными элементами корпусов



Актуальные издания




PD CLC/TS 50701:2023

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CLC/TS 50701

August 2023

ICS 35.030; 45.020

Supersedes CLC/TS 50701:2021

English Version

Railway applications - Cybersecurity

Applications ferroviaires - Cybersécurité

Bahnanwendungen - Cybersecurity

This Technical Specification was approved by CENELEC on 2023-06-19.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

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

CENELEC

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. CLC/TS 50701:2023 E

Спасибо за внимание!